GREGORY J. MADDEN
SUSAN H. POPE
HONG PARK
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Drop CC-9528
Washington, D.C. 20580
Tel: (202) 326-2426, -3302, -2158
Fax: (202) 326-3197
email: gmadden@ftc.gov, spope@ftc.gov,
hpark@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendant.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

I. INTRODUCTION 1

II. LifeLock's Post-Order Business Activities 3

A. LifeLock Claimed It Protected Consumers' Personal Information At or Above Industry Standards. 3

B. LifeLock's Information Security Suffered Critical Weaknesses. 6

1. LifeLock Did Not Implement and Maintain an Information Security Program Meeting Minimum Information Security Industry Standards. 6

(a) LifeLock Did Not Manage Security Vulnerabilities from Unpatched and Outdated Software. 10

(1) LifeLock Failed to Implement An Effective and Timely Patch Management System. 10

(2) LifeLock Improperly Downgraded Vendor Patches as "Low" Priority Vulnerabilities. 12

(b) LifeLock's Vulnerability Remediation Management System Was Not Working. 14

(1) LifeLock Did Not Timely Address Known Penetration Test Vulnerabilities for Months, If at All. 14

(2) Statistical Analysis of LifeLock's VRR Logs and LifeLock's Own Documents Amply Demonstrate the Systemic Failures of Its Vulnerability Management Remediation System. 20

(c) LifeLock Did Not Perform Security Evaluations Before Making New Production Systems Operational. 24

(d) LifeLock Did Not Perform All Required Scans Necessary to Protect Consumers' Information. 26

(e) LifeLock Did Not Document it Compliance. 27

2. LifeLock Needed More InfoSec Staff. 28

C. LifeLock Advertised "Relentless" "24/7" Protection. 29

1. LifeLock Systematically Delayed Credit Inquiry Alerts. 32

2. LifeLock Suppressed Bank Account Alerts on Weekends. 33

3. LifeLock Did Not Send Alerts During "Planned Maintenance" Activities. 34

III. DISCUSSION 34

A. LifeLock Violated the Order. 34

1. LifeLock Violated the Order's Information Security Provision. 35
2. LifeLock Misrepresented Its Protection of Consumers' Personal Information. 41
3. LifeLock Also Misrepresented Its Identify Theft Protection Services. 43
4. LifeLock Violated the Order's Recordkeeping Requirements. 45
B. Consumers Are Entitled to Redress 46
IV. CONCLUSION 48

TABLE OF AUTHORITIES

Cases

Ahearn ex rel. NLRB v. Int'l Longshore & Warehouse Union, Locals 31 & 24, 721 F.3d 1122 (9th Cir. 2013) 46

FTC v. Affordable Media, LLC, 179 F.3d 1228 (9th Cir. 1999) 35

FTC v. BlueHippo Funding, LLC, 762 F.3d 238 (2d Cir. 2014) 46, 47, 48

FTC v. Bronson Partners, LLC, 654 F.3d 359 (2d Cir. 2011) 48

FTC v. EDebitPay, LLC, 695 F.3d 938 (9th Cir. 2012) 46

FTC v. Figgie Int'l, 994 F.2d 595 (9th Cir. 1993) 46, 47

FTC v. Kuykendall, 371 F.3d 745 (10th Cir. 2004) (*en banc*) 46, 47, 48

FTC v. Pantron I Corp.,33 F.3d 1088 (9th Cir. 1994) 47

In the Matter of Thompson Medical Co., 104 F.T.C. 648, 1984 FTC LEXIS 6 (November 23, 1984) *aff'd Thompson Medical Co., Inc. v. FTC*, 791 F.2d 189 (D.C. Cir. 1986) 47

McComb v. Jacksonville Paper Co., 336 U.S. 187, 69 S. Ct. 497, 93 L. Ed. 599 (1949) 46

McGregor v. Chierico, 206 F.3d 1378 (11th Cir. 2000) 46

Shillitani v. United States, 384 U.S. 364, 86 S. Ct. 1531, 16 L. Ed. 2d 622 (1966) 34

United States v. United Mine Workers, 330 U.S. 258, 67 S. Ct. 677, 91 L. Ed. 884 (1947) 46

TABLE OF EXHIBITS

Ex. 1, Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants LifeLock and Davis (D.E. #9, March 15, 2010).

Ex. 2, Federal Trade Commission, Complaint for Permanent Injunction and Other Equitable Relief, filed in *FTC v. LifeLock, Inc.*, No. 10-0530-PHX (D. Ariz.) (D.E. #1, March 9, 2010).

Ex. 3, *PCI Report on Compliance for LifeLock*, (b)(3):6(f),(b)(4) July 2013.

Ex. 4, LifeLock Montel Williams Infomercials.

Ex. 5, Letter from Andrew Berg, Greenberg Traurig, LLP to Susan Pope, Federal Trade Commission (April 7, 2015).

Ex. 6, Declaration of David Hendrickson, Investigator, Federal Trade Commission (Sept. 16, 2014) with Exhibit A, LifeLock Website, Nov. 5, 2013.

Ex. 7, Exhibit B to Hendrickson Declaration, LifeLock Website, August 18, 2014.

Ex. 8, *LifeLock Frequently Asked Question, How do I know my information is secure with LifeLock?* July 14, 2015, *https://lifelock.custhelp.com/app/answers/detail/a_id/149.*

Ex. 9, LifeLock direct mail advertisements.

Ex. 10, LifeLock direct mail advertisements.

Ex. 11, LifeLock direct mail advertisements.

Ex. 12, Trademark Reg. No. 4165114, *Relentlessly Protecting Your Identity.*

Ex. 13, LifeLock Short Form television advertisements.

Ex. 14, *LifeLock, Inc. Risk Assessment Overview*, internal LifeLock risk assessment excel spreadsheet.

Ex. 15, *2013 Risk Assessment Report, Last Update April 15, 2013,* internal LifeLock risk assessment excel spreadsheet.

Ex. 16, *PCI DSS Gap Analysis Report for LifeLock*, (b)(3):6(f),(b)(4) (May 21, 2013).

Ex. 17, Letter from Andrew G. Berg, Greenberg Traurig, LLP to Gregory J. Madden, Federal Trade Commission (Dec. 24, 2014).

Ex. 18, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, (Dec. 9, 2014).

Ex. 19, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (Jan. 2, 2015).

Ex. 20, Expert Report of Dr. Eric B. Cole.

Ex. 21, Adobe Security Bulletins, *https://helpx.adobe.com/security/products/flash-player/apsb14-13.html*.

Ex. 22, Email from Gwen Ceylon to Tony Valentine, Subject: The thinks that make me shake my head (Jan. 7, 2013).

Ex. 23, LifeLockVulnerability Remediation Request email.

Ex. 24, *LifeLock, Inc., PCI Augmented Audit Check List*, June 7, 2013.

Ex. 25, *LifeLock, Inc., PCI Audit Check List*, April 19, 2013.

Ex. 26, Email from (b)(3):6(f),(b)(4) to multiple recipients, Subject: VRR Process Changes (July 1, 2013).

Ex. 27, Payment Card Industry Data Security Standard, Version 2.0.

Ex. 28, (b)(3):6(f),(b)(4) *LifeLock Security Review* (September 21, 2012).

Ex. 29, (b)(3):6(f),(b)(4) *LifeLock, Inc., Information Assurance Services Enterprise Security Assessment* (November 13, 2012).

Ex. 30, Email from Gwen Ceylon to Tony Valentine, Subject: Pen Tests Remediation Plan.xlsx (January 4, 2013).

Ex. 31, Email from (b)(3):6(f),(b)(4) to Rich Stebbins, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) Renee Ramirez, Subject: PLEASE READ FOR APPROVAL OR FURTHER DISCUSSION: Vulnerability Remediation and Patch Management – for PCI Readiness (March 6, 2013).

Ex. 32, Declaration of Elizabeth A. Miles.

Ex. 33, multiple LifeLock Vulnerability Remediation Request emails.

Ex. 34, multiple LifeLock Vulnerability Remediation Request emails.

Ex. 35, multiple LifeLock Vulnerability Remediation Request emails.

Ex. 36, Email from (b)(3):6(f),(b)(4) to David Bridgeman, AnneMarie Olson, Michael Peters, cc: Tony Valentine, Subject: Pen Test and Remediation Internal Conversation from Cristy for PCI (July 16, 2013).

Ex. 37, Email from (b)(3):6(f),(b)(4) to (b)(3):6(f),(b)(4) Brian Kao, cc: Connie Suoo, Tony Valentine, (b)(3):6(f),(b)(4) Subject: Urgent Request: PCI Evidence Gathering – (b)(3):6(f),(b)(4) Ticket 81911 (July 16, 2013).

Ex. 38, Email from Anne Marie Olson to Michelle Grant, (b)(3):6(f),(b)(4) Subject: Security Vulnerabilities (October 11, 2013).

Ex. 39, Email from Austin Appel to (b)(3):6(f),(b)(4) Subject: Outstanding Penetration Test issues (November 5, 2013).

Ex. 40, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (Sept. 19, 2014).

Ex. 41A & B, excerpts from Vulnerability remediation log reports.

Ex. 42, *Security Exception Risk Acceptance Form*, RAF 001 (April 18, 2013).

Ex. 43, Email from (b)(3):6(f),(b)(4) to AnneMarie Olson, Subject: Re: RAF001 Lack of Antivirus on Metranet Server(s) (April 17, 2013).

Ex. 45, Excerpts from *PCI Report on Compliance for LifeLock*, (b)(3):6(f),(b)(4) October 2014.

Ex. 46, Email from Gwen Ceylon to Jim Shoemaker: Andrew Ureta, Subject: Here's all your Documents and Findings on Your Systems for You to Review/Update and Remediate, with attachment, Pre-PCI 2013 Remediation Task List.

Ex. 47, Email from Gwen Ceylon to (b)(3):6(f),(b)(4) Subject: PCI Environment Full Vulnerability CSV Report January Scan.xlsx (January 17, 2013).

Ex. 48, Email from Karen Overton to (b)(3):6(f),(b)(4), Subject: Updated SOPs (March 22, 2013).

Ex. 49, Email from Austin Appel to Mike Wan, (b)(3):6(f),(b)(4), Brain Kao, Subject: Web-based vulnerabilities (Jan. 3, 2014).

Ex. 50, Email from (b)(3):6(f),(b)(4) Subject: FW: Requests Over 150 Days Still Open (Aug. 1, 2014).

Ex. 51, Email from Gwen Ceylon to Jenner Holden, Subject: RE: RA (November 15, 2012).

Ex. 52, Email from (b)(3):6(f),(b)(4) to Scott Watson, David Bridgman, Subject: InfoSec Scans (March 19, 2013).

Ex. 53, Email from (b)(3):6(f),(b)(4) to Anne Marie Olson, Austin Appel, Subject: Final Thoughts/Comments/Info (July 25, 2013).

Ex. 54, Email from (b)(3):6(f),(b)(4) to AnneMarie Olson, Subject: RE: Change Management Standard, (February 11, 2014).

Ex. 55, Email from (b)(3):6(f),(b)(4) to Tony Valentine, Subject: RE: ROC – Updated list of Critical and Post-ROC Items – Version 3 (July 15, 2013).

Ex. 56, Letter from William C. MacLeod, Kelley Drye & Warren, LLP, to Susan Pope, Federal Trade Commission (June 12, 2015).

Ex. 57, LifeLock "decommissioned server" spreadsheet produced with Ex. 56.

Ex. 58, Email from Jenner Holden to Patrick Pendleton, Subject: Q4 Staffing (September 26, 2013) LIFELOCK-0089026-27.

Ex. 59, *2013 Risk Assessment Report, Last Updated April 15, 2013*,excel spreadsheet.

Ex. 60, Email from (b)(3):6(f),(b)(4) to Brian Kao, Subject: Refer-a-Friend Release into Stage (November 13, 2013).

Ex. 61, *Peters v. LifeLock, Inc. et al.*, 14-cv-00576-ROS, Cmpl. ¶¶ 16, 18-21, 31 D.E. #1 (D. Ariz. March 2, 2014).

Ex. 62, *FTC Mandated Independent Assessment of LifeLock Information Security Program, Third Reporting Period 9/16/2012 – 9/15/2014*, (b)(3):6(f),(b)(4) (September 23, 2014).

Ex. 63, Letter from Andrew G. Berg, Greenberg Traurig, LLP to Gregory J. Madden, Federal Trade Commission (Mar. 11, 2015).

Ex. 64, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (Mar. 31, 2014).

Ex. 65, Declaration of Steve Seoane, Chief Product Officer, LifeLock, Inc., (March 6, 2015).

Ex. 67, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (July 2, 2014).

Ex. 68, *LifeLock, Inc. Internal Audit, 2013 Internal Audit Plan*, LifeLock PowerPoint Presentation (Feb. 21, 2013).

Ex. 69, Email from Gwen Ceylon to Tony Valentine, Subject: 2012 RA Workbook – Update 12192012.xlsx (Dec. 20, 2012).

Ex. 70, Letter from Andrew G. Berg, Greenberg Traurig, LLP to Gregory J. Madden, Federal Trade Commission (October 22, 2014).

Ex. 71, *DLA Piper, LLC - Digital Forensic Investigation Report*, (b)(3):6(f),(b)(4) (Nov. 26, 2014).

Ex. 72, FTC Letter from Gregory Madden, Federal Trade Commission, to Andrew Berg, Greenberg Traurig, LLP (March 13, 2014).

Ex. 73, Declaration of Vinayak Balasubramanian (July 20, 2015).

I. INTRODUCTION

LifeLock, Inc. ("LifeLock") violated this Court's March 15, 2010 Permanent Injunction Order[1] by failing to establish, implement, and thereafter maintain a comprehensive information security program. Instead, LifeLock's information security program fell below even minimum information security industry standards. LifeLock compounded this failure by misrepresenting the protection it provided for customers' highly sensitive personal information. Additionally, LifeLock misrepresented its identity theft protection service claiming relentless 24/7 monitoring and alerting when, in fact, there were multiple gaps in the promised services.

Moreover, LifeLock did not implement even basic elements of a well-designed information security program, unilaterally downgrading the importance of patches; failing to apply critical and readily available system patches for months at a time; failing to timely remediate, losing track of, and failing to remediate, high priority system vulnerabilities for months, and in some instances almost two years; failing to scan new production systems for security vulnerabilities before making them operational; and failing to perform required vulnerability scans on all its systems that contained members' credit card information. These failures led to a successful 2014 "ransomware" attack that infiltrated LifeLock's system and denied it access to some of its own consumer files.

[1] Ex. 1, D.E. #9, Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants LifeLock and Davis ("Order").

All the while, LifeLock misrepresented that it protected consumers' personal information at the highest levels like at financial institutions, that it was meeting Payment Card Industry Data Security Standards (PCI DSS), and assuring consumers it would "Protect Your Identity," guard your "social security number," and "No One" protected your identity better.

Additionally, in advertisements dramatically depicting the dangers of identity theft, LifeLock unmistakably and unequivocally trumpeted its identity theft protection service as 24/7, every minute of every day, alerting customers "as soon as" it detected a threat in its network. In reality, LifeLock did not have 24/7 alerting capabilities for credit inquiry alerts, did not process bank account alerts on weekends for eight months, and delayed alerts during planned maintenances on its alert system computers.

These failures violate the Order LifeLock entered pursuant to the complaint the FTC filed in March 2010. That suit alleged that LifeLock's data system was vulnerable, LifeLock did not employ "reasonable and appropriate measures" protecting customers' personal information, and LifeLock misrepresented its identify theft protection services.[2] The parties concurrently filed an Order settling the case, which prohibited LifeLock from: failing to protect consumers' personal information with a comprehensive information security program (Section II); misrepresenting its protection of consumers' personal information (Section I.B); misrepresenting the means, methods, procedures, effects, effectiveness, coverage, or scope of its identity protection services (Section I.A); and failing to create and retain all records necessary to document its

[2] Ex. 2, Cmpl. ¶¶ 17-20, 23-34, 35-37, D.E. #1.

Order compliance (Section VIII.A.7).[3] Because LifeLock's actions violated these core Order provisions customers are legally entitled to a refund for each month that LifeLock did not deliver on its promises.

II. LifeLock's Post-Order Business Activities

A. LifeLock Claimed It Protected Consumers' Personal Information At or Above Industry Standards.

LifeLock, through its post-Order advertisements, claimed it was meeting PCI DSS standards;[4] protected consumers' personal information at the highest level, equivalent to that of financial institutions; and that "No One" protected consumers from identity theft better. Indeed, "a fundamental component" of LifeLock's identity theft protection business is securing its customers' information and doing so at a "greater level" than companies not in the identity theft protection business.[5]

Specifically, LifeLock flooded television airwaves with infomercials claiming its high level of protection for consumers' personal information.[6] In two infomercials,

---

[3] Ex. 1, Order, D.E. #9.

[4] The Payment Card Industry Data Security Council, founded by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., developed the PCI DSS as the technical requirements of each of their data security compliance programs that merchants must satisfy. *See https://www.pcisecuritystandards.org/organization_info/.*

[5] *See* Ex. 3, *PCI Report on Compliance for LifeLock*, (b)(3):6(f),(b)(4) July 2013, LIFELOCK-0097021-229, 0097023. The FTC is providing the full Bates range cite for LifeLock documents cited herein, but the attached Exhibits may be excerpted and/or redacted versions.

[6] Ex. 4, LifeLock Montel Williams Infomercials, LKOC1024_LIFELOCK_MONTEL_V1_2_25_13_VANITY STOP.mp4 (Ref. 137); LKOC1044_MONTEL_2.0_STOP_LOC1044_VANITY.mov (Ref. 138); LKOC1067_MONTEL_2.5_STOP_2.5_STOP_ LKOC1067_122913_small.mp4 (Ref. 139); and LKOC1060_MONTEL_2.5_HOLIDAY_VANITY.mp4 (Ref. 140). LifeLock

celebrity Montel Williams and LifeLock CEO Todd Davis stand in front of a thick glass wall looking into LifeLock's customer call center as Davis explains:

> [W]e take security very seriously. **In fact, we meet the high levels of security data handling, PCI level 1. These are the same kind of certifications that your financial institutions have. So we have to make sure that that data of those members does not get out.** We can't even tape audio there in our Command Center.[7]

(Emphasis supplied.) The Montel Williams infomercials with PCI Level 1 certification and financial institution level information security claims aired **over 48,000** times from 2010 through March 26, 2015.[8]

LifeLock's website reinforced its alleged high level information security, assuring consumers it was "safeguarding the Personal Information of [its] members."[9] It repeatedly claimed it met PCI DSS standards,[10] including consistently hyping its "credentials" as "Level 1 compliant under the Payment Card Industry Data Security Standard."[11] Moreover, the "Frequently Asked Questions" on its current

---

produced advertisements and assigned reference numbers to the advertisements and for ease of identification the FTC is utilizing those reference numbers in this filing.

[7] Ex. 4, Ref. 137 at 16:03 and Ref. 138 at 17:18; *see also* Ref. 139 at 17:48 and Ref. 140 at 17:49.

[8] *See* Ex. 5, Letter from Andrew Berg, Greenberg Traurig, LLP to Susan Pope, Federal Trade Commission, (April 7, 2015) LIFELOCK-0134767-69, 0134767-68 and Annex 2 LIFELOCK-0135515 and Ex. 73, Declaration of Vinayak Balasubramanian ("Balasubramanian Decl.") ¶ 42, Exhibit J (July 17, 2015).

[9] Ex. 6, Declaration of David Hendrickson, Investigator, Federal Trade Commission (Sept. 16, 2014) with Exhibit A, LifeLock Website, Nov. 5, 2013, *http://www.lifelock.com/* captured at [11/5/2013 2:40:01 PM] FTC000001-674, 0000025 *see also* Ex. 7, Exhibit B to Hendrickson Declaration, LifeLock Website, August 18, 2014, *http://www.lifelock.com* captured [8/18/2014 9:20:04 AM], FTC-0000675-2008, 0000711

[10] Ex. 6, at FTC-0000029; Ex. 7, at FTC-0000715.

website assures consumers it maintains "a high level of protection of member data" and is "compliant as a Level 1 merchant under the PCI-DSS."[12]

Finally, LifeLock fortified these claims through its ubiquitous advertising. Its trademarked tagline was, "Relentlessly Protecting Your Identity."[13] It repeatedly claimed "No One Protects You Better Than LifeLock,"[14] and that it provided the "most comprehensive identity theft protection" available,[15] guarding a consumer's "social security number"[16] and telling consumers it would "Protect Your Identity."[17]

---

[11] Ex. 6, at FTC-0000062; Ex. 7, at FTC-0000755. Under PCI Level 1, evaluation of PCI DSS compliance must be performed by a third party rather than an internal assessor.

[12] Ex. 8, *LifeLock Frequently Asked Question, How do I know my information is secure with LifeLock,?* July 14, 2015, *https://lifelock.custhelp.com/app/answers/detail/a_id/149*, FTC-0002202; *see* Ex.73, Balasubramanian Decl. ¶ 41.

[13] Ex. 12, Trademark Reg. No. 4165114, "Relentlessly Protecting Your Identity," at FTC-0002086; *see, e.g.*, Ex. 4, Ref. 137 at 10:46 and 28:26; Ref. 138 at 12:00 and 29:41; Ref. 139 at 10:42 and 28:35; Ref. 140 at 10:42 and 28:35; Ex. 6, at FTC-0000004, FTC-0000006, FTC-0000008, FTC-0000014, FTC-0000019, FTC-0000071; Ex. 7, at FTC-0000675-76, FTC-0000745, FTC-0000917; Ex. 9, LIFELOCK-0132739-43 (direct mail)(Ref. 144); LIFELOCK-0132855-60 (direct mail)(Ref. 165); Ex. 10, LIFELOCK-0133006-11 (direct mail) (Ref. 194); LIFELOCK-0133109-0133111 (direct mail) (Ref. 214); Ex. 11, LIFELOCK-0133365-70 (direct mail)(Ref. 266); LIFELOCK-0133458-62 (direct mail) (Ref. 286); and LIFELOCK-0133607-10 (direct mail) (Ref. 317).

[14] *See, e.g.*, Ex. 13, LifeLock Short Form Television advertisements, ZTVT4783_LL_HOLIDAY_2012.mp4 at 1:33 (Ref. 106); ZTVT4783_LL_HOLIDAY_2013.mov at 1:13 (Ref. 107); ZTVT4727 bn_PLdoc120_ZTVT4727 uniqueURL_OnGuard 960x540.mp4 at 1:20 (Ref. 122); ZTVT4946 PARALLEL LIVES OPT W-GIU DOCTOR_130806_H264.MP4, at 1:16 (Ref. 123).

[15] *See, e.g.*, Ex. 4, Ref. 137 at 19:30, and 28:05; Ref. 138 at 11:55; Ref. 139 at 10:38; Ex. 13, LKOC1001H FFult120v10 LKOC1001H vanity.mp4, at :30 (Ref. 112); ZTVT4944_PL_Orig_opt_w_Giuliani_120_ ZTVT4944_Vanity.mp4, at :26 and :49 (Ref. 116); Ref. 122 at :44; LKOC1034H PLsoc60 LKOC1034H vanity.mp4 at :33 (Ref. 128); Ex. 6, at FTC-0000048, FTC-0000069, and FTC-0000073-74; Ex. 7, at

In fact, LifeLock had numerous significant deficiencies in its information security program, making a mockery of such claims. Internal emails and documents, third party reports, and Dr. Eric Cole's expert report establish not only that LifeLock failed to establish, implement, and thereafter maintain a comprehensive information security program at the high level it claimed, but, shockingly, that it failed to meet even the minimum industry standards for a business of its kind and size.

B. LifeLock's Information Security Suffered Critical Weaknesses.

To provide its identity theft protection service, LifeLock obtained its members' sensitive personal information (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) [18] The Order requires LifeLock to protect this sensitive information with a comprehensive information security program. Such a comprehensive information security program requires proactive assessments, issue tracking, and timely addressing any identified deficiencies and vulnerabilities.[19] LifeLock's system did not even come close.

1. LifeLock Did Not Implement and Maintain an Information Security Program Meeting Minimum Information Security Industry Standards.

Multiple internal assessments flagged LifeLock's information security weaknesses, yet it did not take timely steps to fix them. For example, in February 2013,

---

FTC-0000747, FTC-0000750, and FTC-0000754; *see also* Ref. 137 at 12:26; Ref. 138 at 13:40, 20:43, and 29:21

[16] *See, e.g.*, Ex. 13, Ref. 116 at :53; LKOC1055H_LifeLock_PLmary60_LKOC1055H_vanity.mp4 at :33 (Ref. 120); Ref. 122 at 1:13; Ref. 128 at :34.

[17] *See, e.g.*, Ex. 13, Ref. 116 at :53; Ref. 120 at :33; Ref. 122 at 1:13.

[18] Ex. 6, at FTC-0000032.

[19] Ex. 20, Expert Report of Dr. Eric B. Cole ("Cole Rpt.") ¶ 49.

almost three years after entry of the Order, LifeLock's Internal Auditor presented the Board of Director's Audit Committee with a Risk Assessment identifying the company's high risk areas. The auditor described LifeLock's IT "Enterprise Security" risks as "Lack of overall security strategy for compliance, access management issues, no threat analysis, no configuration standards"[20] and scored company-wide Enterprise Security as LifeLock's highest actual risk, scoring a 3.0 because "controls are not consistently followed or are not in place."[21] IT-Applications/Database risks scored a 2.9 due to risks from "No change management, no patch management, poor data quality or integrity, access management issues."[22]

That internal report was apparently derived from an outside consultant's early 2013 risk assessment highlighting LifeLock's multiple high risk issues, including a high number of critical and exploitable vulnerabilities, as well as system changes made without adhering to the change control management procedures.[23] The consultant's

---

[20] Ex. 14, *LifeLock, Inc. Risk Assessment Overview*, LIFELOCK-0051793-002, "Sorted 2013 RA" Worksheet; *see also* Ex. 68, *LifeLock, Inc. Internal Audit, 2013 Internal Audit Plan*, (Feb. 21, 2013), LifeLock PowerPoint Presentation, LIFELOCK-0051795-1-19, 0051795-9.

[21] Ex. 14, LIFELOCK-0051793-002. The assessment scored risks on a 1 to 4 point scale, 3 representing "Risk is high as controls are not consistently followed or are not in place," and 2 representing "Risk is medium as existing controls are in place but not formally documented or tested." *Id.*

[22] *Id.*

[23] Ex. 69, Email from Gwen Ceylon to Tony Valentine, Subject: 2012 RA Workbook – Update 12192012.xlsx (Dec. 20, 2012), ("Sorted RPN 2012" worksheet), LIFELOCK-0084027-28, 0084028-003. *See also*, Ex. 15, *2013 Risk Assessment Report, Last Update April 15, 2013*, ("Sorted RPN 2012" worksheet), LIFELOCK-0075439, 0075439-002. LifeLock identified LIFELOCK-0075439 as an internal information security risk assessment. Ex. 70, Letter from Andrew G. Berg, Greenberg Traurig, LLP

action plan warned LifeLock that "P&T Management and staff need to take vulnerability and patch management more seriously and ensure that VRR's [Vulnerability Remediation Request tickets] are submitted and worked to remediate vulnerabilities" as well as to "[e]nforce the Change Control Management Procedure" to ensure changes are tested before they are put into production.[24] (b)(3):6(f),(b)(4) (b)(3):6 (f),(b)(4) an outside reviewer, confirmed this analysis and identified still more security issues (*e.g.*, security standards not maintained or regularly updated, standards not meeting vendor recommended guidelines.)[25]

Despite these admonitions, LifeLock continued to fail to patch, update, scan, monitor, and properly configure its systems. This failure led to a successful September 2014 "ransomware" attack. The hacker compromised LifeLock's system, encrypted certain of its files so LifeLock could not access them, and demanded a ransom payment for a decryption key.[26] That attack succeeded because LifeLock was using long-

---

to Gregory J. Madden, Federal Trade Commission, (October 22, 2014), LIFELOCK-0134032-49, 0134046.

[24] Ex. 69, LIFELOCK-0084028-002 (clarification supplied). *See also*, Ex. 15, LIFELOCK-0075439-002.

[25] Ex. 16, *PCI DSS Gap Analysis Report for LifeLock*, (b)(3):6(f),(b)(4) (May 21, 2013) LIFELOCK-0095891-959, 0095896.

[26] Ex. 18, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, (Dec. 9, 2014), LIFELOCK-0134215-216, 0134216. The attack resulted in LifeLock losing access to 254 consumers' remediation case files. Because LifeLock could not access the files, it is unable to specifically identify the personal information in those files. However, such files contain consumer personal information that often includes (b)(3):6(f),(b)(4) Ex. 17, Letter from Andrew G. Berg, Greenberg Traurig, LLP to Gregory J. Madden, Federal Trade Commission (Dec. 24, 2014) LIFELOCK-0134217-223, 0134217-219.

outdated Adobe Flash software,[27] Adobe Flash 12.0.0.4 - three versions behind the then-most current available, Adobe Flash 15.[28] Indeed, Adobe issued a Security Bulletin on April 28, 2014 urging users to update to at least Flash Player 13.0.0.206 because earlier versions had a "critical vulnerability" susceptible to malicious code. Adobe rated the update a Priority 1, recommending that "administrators install the update as soon as possible. (for example **within 72 hours**)."[29] (Emphasis supplied.)

LifeLock did not heed this warning, failing to update this software **for six months** because its automated deployment system for Windows updates and patches was not working.[30] LifeLock apparently did not even notice this deployment problem for five months.[31] Even then, it did not fix the Adobe vulnerability for almost another month, and then only after it became aware of the ransomware attack.[32]

Moreover, although the ransomware attack occurred on September 23, 2014, LifeLock did not detect it until November 4, 2014 due to additional failures.[33] Specifically, LifeLock's daily monitoring systems never alerted it to the attack because LifeLock's misconfigured daily vulnerability scan program did not detect the older

---

[27] Ex. 19, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (Jan. 2, 2015) LIFELOCK-0134224-40, 0134231 and Ex. 18, at LIFELOCK-0134216.

[28] Ex. 19, at LIFELOCK-0134229; Ex. 20, Cole Rpt. ¶¶ 163-64. *See* Ex. 71, *DLA Piper, LLC - Digital Forensic Investigation Report*, (b)(3):6(f),(b)(4) (Nov. 26, 2014) LIFELOCK-0135499-510, 0135509.

[29] Ex. 21, Adobe Security Bulletins, FTC-0002088-93,0002092 *https://helpx.adobe.com/security/products/flash-player/apsb14-13.html*.

[30] *See* Ex. 19, at LIFELOCK-0134231.

[31] *Id.*

[32] *Id.*

[33] *Id.*

Adobe Flash software.[34] Indeed, LifeLock discovered the attack only after a LifeLock employee could not open a file and reported it to the service desk.[35]

Overall, LifeLock did not: (1) adequately patch and update its systems; (2) track identified security vulnerabilities; (3) perform vulnerability scans before making new systems operational; or (4) perform all PCI mandated scans for merchants handling credit card holder's financial information. Compounding these failures, LifeLock cannot document its Order compliance as required.

As a result, LifeLock's information security program did not meet even minimum information security industry standards, leaving its systems vulnerable and its consumers' personal information exposed.

(a) LifeLock Did Not Manage Security Vulnerabilities from Unpatched and Outdated Software.

LifeLock's patching program had at least two fatal, systematic deficiencies from at least September 2012 to July 2013. First, LifeLock was woefully deficient in identifying, timely remediating, and documenting its patch management issues and resolutions. Second, prior to July 2013, LifeLock improperly downgraded the urgency rating of vendor issued system patches.

(1) LifeLock Failed to Implement An Effective and Timely Patch Management System.

A patch is a vendor issued software fix for remediating an exposure or vulnerability in its software. When a vendor releases a patch, it puts both users and

[34] *Id.* at LIFELOCK-0134232.
[35] *Id.* at LIFELOCK-0134225.

attackers on notice of the vulnerability.[36] Thus, it is critical to apply the patch quickly.[37] PCI DSS requires that critical patches be applied no more than 30 days after the patch's release to the public.[38] Financial institutions apply critical patches within fifteen days.[39]

LifeLock was repeatedly warned that it had significant patching deficiencies, yet did not implement a patch management system addressing those issues for months. In September 2012, a third party review described LifeLock's patching failures as a "high" severity vulnerability and identified web servers using outdated software with "multiple vulnerabilities."[40] Three months later, LifeLock's information security consultant told its Director of Internal Audits these issues still had not been addressed.[41] Two months after that, on March 6, 2013, a new information security consultant told senior LifeLock managers that LifeLock's Windows and Linux systems patching was behind by "at least" three months.[42] An analysis of LifeLock's Microsoft and Linux patching activity

---

[36] Ex. 20, Cole Rpt. ¶ 95.

[37] *Id.* Vendors often provide instructions to patch in much less than 30 days. For example, the Adobe warning about the vulnerability resulting in the successful ransomware recommended application within 72 hours. Ex. 21, at FTC-0002092.

[38] Ex. 27, PCI DSS 2.0, Requirement 6.1, FTC0002094-2168, 0002131. LifeLock's VRR policy, established on July 1, 2013, confirms LifeLock's understanding of this PCI requirement. Ex. 26, Email from (b)(3):6(f),(b)(4) to multiple recipients, Subject: VRR Process Changes (July 1, 2013) LIFELOCK-0053865.

[39] Ex. 20, Cole Rpt. ¶ 170.

[40] Ex. 28, (b)(3):6(f),(b)(4) *LifeLock Security Review*, (September 21, 2012) LIFELOCK-2123-2181, 2137, 2141, 2147; *see also* Ex. 29, (b)(3):6(f),(b)(4) *LifeLock, Inc., Information Assurance Services Enterprise Security Assessment* (November 13, 2012), LIFELOCK-0053403-61, 0053423.

[41] Ex. 30, Email from Gwen Ceylon to Tony Valentine, Subject: Pen Tests Remediation Plan.xlsx (January 4, 2013) LIFELOCK-0038509.

[42] Ex. 31, Email from (b)(3):6(f),(b)(4) to Rich Stebbins, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) Renee Ramirez, Subject; PLEASE READ FOR APPROVAL OR FURTHER

from September 2012 through March 2013 shows LifeLock failed to apply critical Microsoft patches within the required 30 days 56.6% of the time,[43] and applied less than 48% of the Linux non-critical patches within 90 days.[44]

LifeLock's patching records, however, tell only part of the story because they only cover patches LifeLock actually applied and not the universe it should have applied. For instance, during September 2012-March 2013, Microsoft released 17 critical operating system patches. LifeLock had 17 Windows servers in its PCI environment and therefore, should have applied 289 patches (17 servers times 17 patches).[45] LifeLock's patching information, however, shows that it only applied 139, less than half, of these critical operating system patches by the end of March 2013.[46]

(2) LifeLock Improperly Downgraded Vendor Patches as "Low" Priority Vulnerabilities.

Further compounding these problems LifeLock Information Security ("InfoSec") staff unilaterally downgraded system patches, such as Microsoft and Linux, that software vendors rated "critical" or "important," to low priority without any documented justification.[47] In January 2013, LifeLock's information security consultant warned LifeLock's Internal Auditor of this practice, showing him a

---

DISCUSSION: Vulnerability Remediation and Patch Management – for PCI Readiness (March 6, 2013) LIFELOCK-0019638-39.

[43] Ex. 20, Cole Rpt. ¶ 102.

[44] *Id.* at ¶ 104.

[45] *Id.* at ¶ 107.

[46] *Id.*

[47] *See* Ex. 22, Email from Gwen Ceylon to Tony Valentine, Subject: The thinks that make me shake my head (Jan. 7, 2013) LIFELOCK-0038588-89. Moreover, multiple vendor identified patches were included in single remediation tickets, masking the thousands of vulnerabilities as hundreds. *Id.*

Vulnerability Remediation Request (VRR) ticket with multiple critical and severe vulnerabilities that InfoSec staff had submitted as a "low" priority in October 2012.[48] In fact, of the 20 Microsoft patches identified on this VRR, Microsoft ranked 14 "Critical" and 6 "Important," but InfoSec staff downgraded the overall VRR to a "low" priority.[49]

LifeLock's PCI assessor discovered LifeLock's downgrading practice when conducting his PCI DSS review, noting that an InfoSec employee had "unilaterally downgraded [a] Critical patch."[50] As a result, the PCI Assessor required that LifeLock provide evidence that there was now a documented process in place for downgrading a "Critical" vulnerability and that if downgrades had occurred since the implementation of the documented process that LifeLock provide "evidence of the non-unilateral decision."[51] In response, in a July 1, 2013 email to all remediation teams, LifeLock finally announced it was changing the VRR process to eliminate the ability to unilaterally downgrade criticality ratings generated by the automated system scans, instead "using the criticality rating as dictated by the Nexpose service" and only allowing a downgrade upon a formal request with a business justification.[52]

---

[48] *Id.*; *see* Ex. 23, VRR ticket 81561, LIFELOCK-0030131-32.
[49] Ex. 22, at LIFELOCK-0038588; *see* Ex. 23, at LIFELOCK-0030131-32, Ex. 73, Balasubramanian Decl. ¶ 39.
[50] Ex. 24, *LifeLock, Inc., PCI Augmented Audit Check List*, June 7, 2013 LIFELOCK-0039701-07, 0039705. *See also* Ex. 25, *LifeLock, Inc., PCI Audit Check List*, April 19, 2013, LIFELOCK-0009259-61, 0009260 (noting "Main database patches not applies [sic] for some time. Many critical patches over 30 days.. Patch classification downgraded without documented justification.")
[51] Ex. 24, at LIFELOCK-0039705.
[52] Ex. 26, at LIFELOCK-0053865.

(b) LifeLock's Vulnerability Remediation Management System Was Not Working.

LifeLock compounded its patching failures by haphazardly tracking vulnerabilities. An effective vulnerability remediation management process timely and systematically: identifies vulnerabilities, creates remediation tickets, addresses the vulnerabilities, verifies their resolution, and documents the actions addressing the vulnerabilities.[53] LifeLock's vulnerability remediation management system neither systematically nor timely addressed identified vulnerabilities. Therefore, many vulnerabilities remained unremediated for months at a time, and in a number of instances, were closed without any resolution. These systemic deficiencies are demonstrated by both LifeLock's failure to address vulnerabilities identified during third party penetration tests and an analysis of its VRR tickets.

(1) LifeLock Did Not Timely Address Known Penetration Test Vulnerabilities for Months, If at All.

LifeLock's process for addressing vulnerabilities began with creation of a VRR ticket identifying a remediation need. Tellingly, LifeLock failed to remedy the vast majority of VRRs from two third-party penetration tests in September-November 2012 for months, if at all.[54] Indeed, LifeLock lost track of a number of these VRRs more than once.

---

[53] Ex. 20, Cole Rpt. ¶¶ 50-54.

[54] A penetration test is an attempt to compromise a computer system through an authorized attack. The results are used to evaluate infrastructure security and identify security weaknesses. (b)(3):6(f),(b)(4) conducted penetration tests on LifeLock's systems during October-November 2012. Ex. 29, at LIFELOCK-0053407.

The late 2012 (b)(3):6(f), (b)(4) penetration tests resulted in LifeLock's Director of Information Security submitting multiple "high" priority VRRs.[55] Shockingly, LifeLock resolved only one of these high priority penetration test VRRs in less than two months[56] and completely lost track of others. Moreover, LifeLock recognized this fact only when its PCI assessor asked for the remediation documentation.[57]

Specifically, on July 16, 2013, just days before LifeLock "obtained" its annual PCI DSS certification - and 8 to 10 months after these vulnerabilities were identified -

---

[55] Ex. 33, LifeLock Vulnerability Remediation Request emails, VRR 81911, LIFELOCK-0089185; VRR-81913, LIFELOCK-0089109-10; VRR 81915, LIFELOCK-0089212-13; VRR 81916 LIFELOCK-0089214-15;VRR 81926, LIFELOCK-0089223-24; VRR 81932, LIFELOCK-0089225-26; VRR 83219, LIFELOCK-0089119-20; VRR 83232, LIFELOCK-0089186-87. (b)(3):6 (f),(b)(also conducted penetration tests as part of its security review in September 2012 for which LifeLock's Director of Information Security also submitted "high" priority tickets. Ex. 34, VRR 82259, LIFELOCK-0089258; VRR 82261, LIFELOCK-0089259-60;VRR 82263, LIFELOCK-0089261-62; VRR 82267, LIFELOCK-0089263-64;VRR 82269, LIFELOCK-0089330-31;VRR-82271, LIFELOCK-0033794; VRR 82273, LIFELOCK-0089265-66. For both (b)(3):6(f), (b)(4) and (b)(3):6 (f),(b)(4 the priority assigned by LifeLock was sometimes higher and sometimes lower than those assigned by the third party.

[56] Resolving one (b)(3):6(f), (b)(4) and one (b)(3):6 (f),(b)(4 high priority vulnerability in under 30 days. Ex. 35, Email from (b)(3):6(f),(b) (4) to Jenner Holden, Subject: Request id:##81913## has been closed (Nov. 28, 2012) LIFELOCK-0089107-08; Email from (b)(3):6(f),(b) (4) to Jenner Holden, Subject: Request id:##82273## has been closed (Dec. 7, 2012) LIFELOCK-0089336-37.

[57] Ex. 36, Email from (b)(3):6(f),(b)(4) to David Bridgeman, AnneMarie Olson, Michael Peters, cc: Tony Valentine, Subject: Pen Test and Remediation Internal Conversation from (b)(3):6 (f),(b)(4) for PCI (July 16, 2013) LIFELOCK-0073557. To process credit card payments LifeLock needed sign off on its Report on Compliance (RoC) and its Attestation of Compliance (AOC). *See* Ex. 37, Email from (b)(3):6(f),(b)(4) (b)(3):6(f), (b)(4) Brian Kao, cc: Connie Suoo, Tony Valentine, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) Subject: Urgent Request: PCI Evidence Gathering – (b)(3):6(f),(b)(4) Ticket 81911 (July 16, 2013), LIFELOCK-0025172-175, 0025172 ("our previous PCI compliance certification is expired, and our [payment] Processor (b)(3):6 (f),(b)(4 is requesting our new RoC.").

LifeLock employees began looking for evidence that it had addressed them.[58] An internal email to InfoSec department staff and LifeLock's internal auditor reveals: (1) LifeLock had no idea whether any work had been done on the VRRs; (2) LifeLock desperately *hoped* that there had been "some plan;" and (3) LifeLock believed its PCI auditor would "dance around" LifeLock's failure and still provide the PCI RoC:

> Michael and Anne-Marie, if these items were not addressed somehow (through a remediation plan or something like this), then what will suffice for the [PCI] auditor today is a plan to address the findings in the pen test. This will not hold up the RoC. Hoyt [the auditor] tells me that he will **dance around it.**
>
> HOPEFULLY, there was some plan, even if not completely remediated. Dave? Do you know?

(Bold emphasis supplied, capitals original.)[59]

In response, LifeLock frantically spent that day determining whether anything had been done to address the penetration test VRRs. It discovered that, for many, nothing had been.[60] Indeed, six "high" priority VRRs were backlogged and non-prioritized.[61] Nonetheless, the next day, July 17, 2013, LifeLock incredibly presented evidence to the PCI assessor that all of these VRR tickets had been "corrected and retested."[62]

---

[58] Ex. 36, LIFELOCK-0073557.
[59] *Id.*
[60] Ex. 37, LIFELOCK-0025172-75.
[61] *Id.* LIFELOCK-0025172-75 ("Please find the attached xls with all of the security requests that I have on my backlog (initiated by Jenner)."
[62] Ex. 3, at LIFELOCK-0097204-05. Moreover, for all of the (b)(3):6(f), (b)(4) penetration tests, regardless of priority, LifeLock did not provide adequate documentation supporting they had been "corrected and retested." Ex. 20, Cole Rpt. ¶¶ 64-72.

In reality, LifeLock had not resolved these VRRs. In October 2013, three months after LifeLock "passed" its PCI certification, an InfoSec employee email confirms these six VRRs had not been addressed:

> These are vulnerabilities that were identified in assessments completed in September and November 2012 **and should have been remediated months ago**. Unfortunately, the tickets were closed when they were moved to (b)(3):6 so we didn't know …

(Emphasis supplied).[63] In November 2013, another InfoSec employee reiterated that LifeLock had not addressed, or did not know the status of, multiple (b)(3):6(f), (b)(4) and (b)(3):6(f VRRs. He identified 22 penetration test VRRs as "[t]ickets we don't know status on," "[t]ickets that are waiting on us," or "[t]ickets waiting on other teams."[64]

Astoundingly, another ten months later, in September 2014, some still remained unresolved. Specifically, LifeLock now admits four of these "high" priority VRRs[65] were "closed without documentation of evaluation" in August 2014.[66] The failure to

---

[63] Ex. 38, Email from Anne Marie Olson to Michelle Grant, (b)(3):6(f),(b)(4) Subject: Security Vulnerabilities (October 11, 2013) LIFELOCK-0081949-56. Five were (b)(3):6(f), (b)(4) vulnerabilities and one was an (b)(3):6(f) vulnerability. (b)(3):6(f), (b)(4) vulnerabilities were: EAD-61 Vulnerability Fix- Disable AutoComplete (VRR 81911); EAD-63 Vulnerability Remediation- Cookie Settings (VRR 81915); EAD-64 Vulnerability Remediation- HTTP Response Information Disclosure (VRR 81916); EAD-112 Vulnerability Remediation- No Clickjacking Protection (VRR 81932); EAD-60 Vulnerability Remediation - Hidden Directory Enumeration (VRR 81926). The (b)(3):6 (f),(b)(4 vulnerability was EAD-95 Vulnerability Remediation- Reflected XSS (VRR 81953).

[64] Ex. 39, Email from Austin Appel to (b)(3):6(f),(b)(4) Subject: Outstanding Penetration Test issues (November 5, 2013) LIFELOCK-0032898-99.

[65] The four vulnerabilities were ticket numbers VRR Nos. 81911, 81915, 81916, and 81932. *See supra* footnote 55.

[66] Ex. 40, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (Sept. 19, 2014) LIFELOCK-0110772-81, 0110774-76. LifeLock "re-opened" three in September 2014 after the FTC requested documentation regarding their resolution. A fourth, identifying the need to disable auto

address penetration test vulnerabilities is a fundamental information security program deficiency.[67]

For those high priority penetration test vulnerabilities that LifeLock did not lose, it remediated only two (one (b)(3):6(f), (b)(4) and one (b)(3):6 (f),(b) (4)) in less than four months. LifeLock's response to the three highest rated (b)(3):6(f), (b)(4) vulnerabilities is telling: Directory Traversal Arbitrary File Read, Local Administrator Password Reuse, and Default or Guessable Application Server Management Console Password.[68] Each received a (b)(3):6(f), (b)(4) CVSS score of 10,[69] and each was exploited by (b)(3):6(f), (b)(4) in a **successful** attack against LifeLock's systems.[70] The combination of password and Directory Traversal vulnerabilities is particularly troublesome because an easily guessable password used to access one directory can lead to other directories containing

---

complete functions on its web site forms, was "closed" in September 2014. LifeLock claims the disable auto complete "cannot be controlled within the application settings. It is controlled by the user's browser." *Id.*, LIFELOCK-0110774. As our expert explains, this is nonsensical and false. Ex. 20, Cole Rpt. ¶ 70.

[67] Ex. 20, Cole Rep. ¶ 85.

[68] Ex. 29, at LIFELOCK-0053421-23.

[69] *Id.* The Common Vulnerability Scoring System (CVSS) is the metric used by the National Vulnerability Database (NVD) to rate the severity of a vulnerability and is part of the National Institute for Standards and Technology (NIST). For each vulnerability, NVD assigns numeric CVSS scores and corresponding severity rankings of "High," "Medium," and "Low." Vulnerabilities are labeled "High" if a base score of 7.0-10.0, "Medium" if a base score of 4.0-6.9, and "Low" if a base score of 0.0-3.9. *See https://nvd.nist.gov/cvss.cfm.*

[70] Ex. 29, at LIFELOCK-0053421-23, 0053430-40.

sensitive information.[71] Although identified in (b)(3):6(f),(b)(4) November 13, 2012 report, LifeLock took no action on any of these for over four monthsv[72]

Similarly, LifeLock took nearly seven months to respond to (b)(3):6(f),(b)(4) identification of a high severity vulnerability, No Effective Anti-Virus Scanning.[73] In its September 21, 2012 report, (b)(3):6 explained this affected two sets of servers, the MetraNet Windows servers and the Microsoft SQL servers:

> either have no AV [anti-virus] installed or had the real time scanner disabled. As shown below the host did not have the (b)(3):6(f),(b)(4) service installed or enabled.
>
> * * * *
>
> **EXPLOIT SCENARIO:** It was possible during testing to take advantage of this vulnerability to run hacking tools on the servers. This allowed password hashes to be recovered.

(Emphasis original.)[74]

The Metranet billing application servers containing cardholder information were outdated and could not run with anti-virus protection.[75] However, LifeLock did not resolve this fundamental vulnerability until mid-April 2013, almost seven months after

---

[71] Ex. 29, at LIFELOCK-0053437 ("Although the directory traversal initially enabled system exploitation, the reuse of local administrator passwords ultimately enabled the compromise of the domain.")

[72] *See* Ex. 41A, excerpt from vulnerability remediation log reports, LIFELOCK-0138077-78 . The expert report details the significance of this vulnerability and LifeLock's deficient remediation management for these vulnerabilities. Ex. 20, Cole Rpt. ¶¶ 73-84.

[73] Ex. 28, at LIFELOCK-2148.

[74] *Id.* Metranet servers are LifeLock's billing application servers and thus contain cardholder information, including PII. *See* Ex. 3, at LIFELOCK-0097025.

[75] Ex. 42, *Security Exception Risk Acceptance Form*, RAF 001 (April 18, 2013) LIFELOCK-0095646. Ex. 43, Email from (b)(3):6(f),(b)(4) to AnneMarie Olson, Subject: Re: RAF001 Lack of Antivirus on Metranet Server(s) (April 17, 2013) LIFELOCK-0032489.

(b)(3):6 (f),(b)(4) originally identified it.[76] To make matters worse, it appears that LifeLock lost track of (b)(3):6 (f),(b)(4) warnings about the Metranet vulnerabilities and only addressed the problem after rediscovering it during the run up to their 2013 PCI certification.[77] Similarly, it appears LifeLock took almost seven months to address the fact that the Microsoft SQL servers[78] had no anti-virus.[79]

(2) Statistical Analysis of LifeLock's VRR Logs and LifeLock's Own Documents Amply Demonstrate the Systemic Failures of Its Vulnerability Management Remediation System.

LifeLock chronically failed to address VRRs because it poorly managed its VRR system. In January 2013, LifeLock's information security consultant reported:

> **The listed VRRs are past due for remediation of vulnerabilities ranked high.** It will be important to demonstrate to our PCI auditors that we have an effective vulnerability/patch management process in place to meet the PCI requirement of remediating vulnerabilities - critical (high) within 1 month. And timely for all other security patches.
>
> * * * *
>
> **VRR process needs to be improved to ensure timely deployment of critical patches to servers.**

---

[76] *Id.* Moreover, LifeLock never really fixed the problem, instead instituting mitigating controls as a short term solution and identifying replacement of the MetraNet product in 2014 as a long term solution. Even so, although the RAF indicates the servers will be replaced in 2014, the October 2014 LifeLock RoC still has the claim of planned replacement in 2014. Ex. 45, Excerpts from *PCI Report on Compliance for LifeLock*, (b)(3):6(f),(b)(4) October 2014, LIFELOCK-0135732, 0135958-59.

[77] *Id.* Although identified by (b) (3):6(f) seven months earlier, the RAF explained: "During the PCI readiness, it was discovered that anti-virus is not installed or running on the Metranet servers" without reference to the months old (b)(3):6 (f),(b)(4) finding.

(b)(3):6(f),(b)(4)

[79] *See*, Ex. 3, at LIFELOCK-0097078 (identifying patch application on April 10, 2013). Notably LifeLock's VRR logs do not document this installation as part of its response to this vulnerability ticket.

(Emphasis supplied.)[80] On January 17, 2013, LifeLock's information security consultant shared her analysis with LifeLock's Senior Director and the Director of Infrastructure, warning that: the vulnerabilities were masked so that over 4600 vulnerabilities in the PCI environment (most ranked "critical") looked like 200; the VRRs were improperly submitted as "low" priority; and the PCI auditor would have a problem with this because PCI DSS now required resolving critical vulnerabilities within a month:

> Currently there are about 200 VRRs in (b)(3):6(f),(b)(4) – 136 are past due. Now some might say 200 VRRs – 200 vulnerabilities, that's not so bad. **But that's not the reality. Currently there are 4669 vulnerabilities on the systems in the PCI environment. Most of them ranked critical.**
>
> * * * *
>
> Some of the VRRs the security guys enter contain hundreds of vulnerabilities in them. **Plus they set the priority of the ticket to low** – making everyone believe even more it's not such a big deal. But the auditor is not going to like seeing this many critical vulnerabilities **especially since control 6.2 of the PCI DSS is now a requirement that you remediate critical vulnerabilities within a month**.

(Emphasis supplied.)[81] That same day the analysis was shared with LifeLock's Internal Auditor.[82]

The VRR logs confirm LifeLock was downgrading patches. For two periods of over three months, from September 1, 2012 to February 21, 2013, and from March 13,

---

[80] Ex. 46, Email from Gwen Ceylon to Jim Shoemaker: Andrew Ureta, Subject: Here's all your Documents and Findings on Your Systems for You to Review/Update and Remediate, with attachment, Pre-PCI 2013 Remediation Task List, LIFELOCK-0085232, LIFELOCK-0085281.

[81] Ex. 47, Email from Gwen Ceylon to (b)(3):6(f),(b)(4) Subject: PCI Environment Full Vulnerability CSV Report January Scan.xlsx, (January 17, 2013), LIFELOCK-0085248-49.

[82] *Id.*

2013 to June 25, 2013, LifeLock did not identify any critical VRRs and only 2 high VRRs.[83] On June 26-28, 2013, shortly after the PCI assessor identified the need for evidence supporting downgraded tickets, LifeLock suddenly created 83 critical and high VRRs – apparently regrading its vulnerabilities.[84] Requiring documentation of downgrade justifications apparently yielded 83 critical and high VRRs. To address this problem, LifeLock's information security consultant circulated an email announcing a new procedure that LifeLock would now have for downgrading: critical VRRs should be remediated in 30 days, high in 60, and medium and low in 90 days.[85]

An analysis of LifeLock's VRR logs from April 2012 to May 2015 show it systematically failed to meet these standards, confirming there was no effective "vulnerability/patch management process in place" to meet PCI DSS requirements.[86] For no criticality category did LifeLock resolve discovered vulnerabilities in less than 111 days.[87] Even for the lowest rated vulnerabilities, LifeLock's average time for VRR resolution was more than the 90 days LifeLock's policy established.[88] For each

---

[83] Cole Rpt. ¶ 62.

[84] *Id.*; Ex. 73, ¶ 43; Ex. 41B, VRR log excerpt.

[85] Ex. 26, LIFELOCK-0053865. Earlier drafts of this new policy had recommended addressing critical priority VRRs in 48 hours, high in 2 weeks, medium in 4 weeks, and low in 8 weeks. Ex. 48, Email from Karen Overton to (b)(3):6(f),(b)(4) Subject: Updated SOPs (March 22, 2013) LIFELOCK-0018299, 0018311-13.

[86] Ex. 46, at LIFELOCK-0085281-012.

[87] This analysis understates the delays for patch related VRRs because there was also a delay between vendor release and LifeLock discovery.

[88] Ex. 26, at LIFELOCK-0053865.

category, low, medium, high, LifeLock did not meet the PCI DSS requirement of installing critical patch VRRs within 30 days of vendor release.[89]

LifeLock VRR Log Criticality[90]	Mean Days from LifeLock Discovery to VRR Ticket Created	Mean Days From LifeLock Discovery to Resolution	Mean Days From LifeLock Discovery to Documented Complete
Critical	43	148	209
High	43	125	252
Medium	28	111	184
Low	24	122	206

LifeLock's own data on the 220 VRRs that it self-rated as critical show its vulnerability remediation management process failed.[91] LifeLock exceeded the absolute outside 30 day timeframe for remediating critical vulnerabilities for 133 VRRs, or 60.5% of its critical VRRs.[92] Moreover, 80 VRRs, or over 36.4% of the critical VRRs, were not resolved for over 90 days.[93]

Moreover, LifeLock's internal documents show its vulnerability remediation management problems persisted well into 2014.[94] In January 2014, LifeLock was still searching for a VRR procedure to prevent future occurrences because "we already have

[89] Ex. 27, PCI DSS 2.0, Requirement 6.1, FTC-0002131.
[90] Ex. 32, Declaration of Elizabeth A. Miles ¶ 24 ("Miles Decl.")
[91] As explained above, LifeLock downgraded numerous critical VRRs to low, so the 220 understates the number of LifeLock's critical VRRs. However, as the table shows, for VRRs categorized as low, LifeLock was well beyond resolving the vulnerabilities in 90 days.
[92] Ex. 20, Cole Rpt. ¶ 88.
[93] *Id.*
[94] *Id.* at ¶ 90.

the problem of a number of vulnerabilities in the backlog."[95] As late as August 1, 2014, LifeLock still had over 100 "high" or "critical" VRRs that were more than 150 days old.[96]

(c) LifeLock Did Not Perform Security Evaluations Before Making New Production Systems Operational.

From November 2012 through at least February 2014, LifeLock failed to implement a "change management" process to effectively scan new systems for security vulnerabilities. A change management process reviews information security system changes to ensure they are secure when they become operational.[97] A robust change management process is a key component to ensuring systems are constantly secure.[98] In November 2012, (b)(3):6(f), (b)(4) told LifeLock it "should review its change and configuration management procedures to ensure that system hardening is integrated into each step of the change management process."[99] At that time LifeLock's information security consultant told its Director of Information Security: "well defined change management plan not in place, people are not following the process."[100] On March 19, 2013 LifeLock's information security consultant explained to senior LifeLock Infrastructure

[95] Ex. 49, Email from Austin Appel to Mike Wan, (b)(3):6(f),(b)(4) Brain Kao, Subject: Web-based vulnerabilities (Jan. 3, 2014) LIFELOCK-0033450-52, 00033450.
[96] Ex. 50, Email from (b)(3):6(f),(b)(4) Subject: FW: Requests Over 150 Days Still Open, (Aug. 1, 2014) LIFELOCK-0134378-385.
[97] Ex. 20, Cole Rpt. ¶¶ 124-25.
[98] *Id.*
[99] Ex. 29, at LIFELOCK-0053409.
[100] Ex. 51, Email from Gwen Ceylon to Jenner Holden, Subject: RE: RA, (November 15, 2012) LIFELOCK-0088187-88.

employees that major changes had not been scanned in the past, it needed to happen in the future, and there was no process in place ensuring such scans would happen:

> (b)(3):6(f),(b)(4) and (b)(3):6(f),(b)(4) as part of security best practice (**and as part of PCI compliance**) InfoSec will need to scan/review all major changes implemented in the environment. **While this has not occurred consistently in the past, we are putting steps in place to ensure that the scans are part of the process.** Since this is not fully documented and a process vetted (as to what works best in reality) I am asking for a ticket for a scan request at this time. Information Security is working with (b)(3):6(f) Renee on what the best process will be, **not just for your team but for all Infrastructure and Engineering teams when major changes occur.**[101]

(Emphasis supplied.) In May 2013, (b)(3):6(f),(b)(4) found this issue remained unaddressed:

> LifeLock is not performing security scans before major system or code changes are released into the CDE [cardholder data environment] environment.
>
> . . . A system could potentially be active in the CDE environment up to six weeks with security vulnerabilities still in place.
>
> . . . LifeLock should incorporate into its change management process a step that requires a security scan upon implementation into the Stage environment and before implementation into Production environment.[102]

On July 25, 2013, LifeLock's information security consultant again flagged this issue, emailing InfoSec staff: "Change Management – one thing LL is really lacking is having significant changes scanned after they go into production."[103] Amazingly, LifeLock did not develop and approve a Change Management standard until February 2014, at least

---

[101] Ex. 52, Email from (b)(3):6(f),(b)(4) to Scott Watson, David Bridgman, Subject: InfoSec Scans (March 19, 2013) LIFELOCK-0026183.

[102] Ex. 16, LIFELOCK-0095896.

[103] Ex. 53, Email from (b)(3):6(f),(b)(4) to Anne Marie Olson, Austin Appel, Subject: Final Thoughts/Comments/Info. (July 25, 2013) LIFELOCK-0029627.

one and a half years after the problem was first identified by a (b)(3):6(f), (b)(4) penetration test.[104]

(d) LifeLock Did Not Perform All Required Scans Necessary to Protect Consumers' Information.

LifeLock did not run all PCI-required vulnerability scans on its virtual local area networks (VLAN). VLANs are groups of workstations, servers and network devices that appear to be on the same local area network despite their geographical distances.[105] Each is susceptible to attack and must be systematically monitored.[106] PCI DSS requires evidence of quarterly scans for each in-scope PCI VLAN to protect cardholder data from attack.[107] On April 4, 2013, LifeLock began scanning some of its VLANs, over nine months too late. LifeLock's information security consultant announced to its Internal Auditor just days before LifeLock's PCI DSS certification was due that it could not provide the quarterly scanning evidence because ". . . not all PCI vlans were being scanned" and "this is going to be noticed by Hoyt because not all vlans have a year's worth of scans **when they should have** (b)(3):6(f),(b)(4) ".[108] (Emphasis supplied.) The PCI DSS requires four quarterly internal scans in the most recent 12 month period and (b)(3):6(f found in the 2013 PCI RoC that "internal quarterly scans . . . have occurred at

---

[104] Ex. 54, Email from (b)(3):6(f),(b)(4) to AnneMarie Olson, Subject: RE: Change Management Standard, (February 11, 2014) LIFELOCK-0033420-23.
[105] *See http://www.techopedia.com/definition/4804/virtual-local-area-network-vlan.*
[106] Ex. 20, Cole Rpt. ¶¶ 50, 153.
[107] Ex. 27, PCI DSS 2.0, Requirement 11.2.1.a at FTC-0002153; *see also supra* footnote 4 (explaining PCI DSS).
[108] Ex. 55, Email from (b)(3):6(f),(b)(4) to Tony Valentine, Subject: RE: ROC – Updated list of Critical and Post-ROC Items – Version 3, (July 15, 2013) LIFELOCK-0010367-74, 0010367.

least quarterly for the last 12 months."[109] However, LifeLock admits that, in fact, these VLANs had not been scanned before April 4, 2013.[110] LifeLock thus left its customers' credit card information vulnerable between July 2012 and April 2013.

(e) LifeLock Did Not Document it Compliance.

Consistent documentation of activities is critical to an effective information security program.[111] Yet, LifeLock could not produce computer logs documenting the alerts sent from its alerting tool (b)(3):6(f),(b)(4) to its Security Incident and Event Management (SIEM) monitoring tool. These tools monitor LifeLock's systems for intrusion or attacks. These logs are the core component for monitoring and evaluating LifeLock's ability to detect intrusions or attacks as well as its response.[112]

Additionally, LifeLock could not produce patch history logs for its computers for September 2012 through March 2013. Instead, LifeLock had to create patch history logs by pulling the information directly from the available servers.[113] However, for over 550 "decommissioned" servers, LifeLock has no record of when, or if, they were ever patched, or when they were "decommissioned."[114] Without patch history logs, LifeLock does not have sufficient information to evaluate its information security

---

[109] Ex. 3, at LIFELOCK-0097199-200.
[110] Ex. 40, at LIFELOCK-0110780.
[111] Ex. 20, Cole Rpt. ¶¶ 54,97,141-43 and 147.
[112] *Id.* at ¶ 147.
[113] *See* Ex. 56, Letter from William C. MacLeod, Kelley Drye & Warren, LLP, to Susan Pope, Federal Trade Commission (June 12, 2015) FTC-0002169-74, 0002172.
[114] *Id.* at FTC-0002173-74. Notably, the nine servers that were identified as having the most vulnerabilities in January 2013, were all subsequently decommissioned. LifeLock does not have a record of addressing those vulnerabilities. Ex. 47, LIFELOCK-0085250; Ex. 57, LifeLock "decommissioned server" spreadsheet produced with Ex. 56, LIFELOCK-0138076.1-13. Ex. 73, Balasubramanian Decl. ¶ 40.

program, to make necessary adjustments, or to document it is running a comprehensive information security program.

2. LifeLock Needed More InfoSec Staff.

LifeLock's multiple failures were due in part to the fact it had too few people to meet its information security responsibilities. InfoSec personnel raised this issue on multiple occasions. In September 2012, LifeLock's Director of Information Security emailed LifeLock's Chief Information Officer (CIO) explaining that LifeLock had insufficient security staff in place:

> **As we have discussed, I have an immediate need for a Senior Security Analyst FTE.** The position would focus on significantly broadening and deepening our efforts to discover and remediate technical security vulnerabilities in our environment. Currently, we cover our production systems with regular automated vulnerability scans. This is probably about 20% of our systems. . . . **Simply put, our current coverage for discovering system vulnerabilities before the bad guys is not adequate.** For example, the large majority of issues found by the due diligence security audit **were of areas that we have not yet inspected ourselves.**

(Emphasis supplied.)[115] At that time, the Information Security Director also requested two additional full-time employees.[116] In April/May 2013, InfoSec employees identified monitoring activities as unattainable absent additional staffing, saying InfoSec could not monitor recommended account creation, user activity, and inactive

[115] Ex. 58, Email from Jenner Holden to Patrick Pendleton, Subject: Q4 Staffing (September 26, 2013) LIFELOCK-0089026-27, 0089026.
[116] *Id.* at LIFELOCK-0089027.

accounts.[117] In November 2013, LifeLock's CISO commented "It's been a bumpy ride for me without an AppSec person."[118]

Despite these constant warnings, LifeLock did not commit additional resources until after a former employee threatened suit[119] and the FTC began asking questions - 15 months after the Information Security Director told LifeLock's CIO they were only covering "20%" of their system and could not discover "system vulnerabilities before the bad guys."[120] LifeLock did not finally begin augmenting its InfoSec staff, growing from 5 to 15 employees between December 2013 and December 2014 in an attempt to build a comprehensive information security program.[121]

C. LifeLock Advertised "Relentless" "24/7" Protection.

LifeLock sold its identity theft protection services nationwide by advertising a "proactive alert system" notifying customers via email, voicemail, mobile app, and/or text when their personal information appeared in applications for credit or services: "We alert you **whenever** we detect your personal information being used to apply for

---

[117] Ex. 59, *2013 Risk Assessment Report, Last Updated April 15, 2013*, LIFELOCK-0043045-001 to 005, 0043045-001, see "4/01/13amo" in Notes/References column.

[118] Ex. 60, Email from (b)(3):6(f),(b)(4) to Brian Kao, Subject: Refer-a-Friend Release into Stage (November 13, 2013) LIFELOCK-0033750-52, 0033750.

[119] Notably, Michael Peters, hired as LifeLock's CISO for a short period of time (29 days in July 2013), is suing LifeLock and alleges, *inter alia*, that LifeLock had serious information security deficiencies and "[a] large part of this problem was staffing." Ex. 61, *Peters v. LifeLock, Inc. et al.*, 14-cv-00576-ROS, Cmpl. ¶¶ 16, 18-21, 31 D.E. #1 (D. Ariz. March 2, 2014), FTC-0002175-90 .

[120] Ex. 58, at LIFELOCK-0089026.

[121] *See* Ex. 62, *FTC Mandated Independent Assessment of LifeLock Information Security Program, Third Reporting Period 9/16/2012 – 9/15/2014*, (b)(3):6(f),(b)(4) (September 23, 2014) LIFELOCK-0133853-939, 0133860; Ex. 63, Letter from Andrew G. Berg, Greenberg Traurig, LLP to Gregory J. Madden, Federal Trade Commission (Mar. 11, 2015), LIFELOCK-0134680-8, 0134682.

wireless services, retail credit, utilities, and mortgage loans within our extensive network."[122] (Emphasis supplied.) LifeLock repeatedly claimed it "continuously monitor[s]" for threats and it notifies its customer **"[a]s soon as** we receive any indication that your personal information has been compromised." (Emphasis supplied.)[123]

The *sine qua non* of LifeLock's advertising was that it would catch and immediately alert its customers about threats to their identity. Indeed, in June 2010, LifeLock trademarked the phrase "Relentlessly Protecting Your Identity" and used it through at least December 2014.[124] Moreover, LifeLock emphasized the importance of immediate notification to protect against identity theft.[125] For example, LifeLock's television advertisements dramatically depicted the dangers of identity theft, showing nefarious characters stealing consumers' identities and draining their bank accounts. Its advertisements claimed "24/7" vigilance and consumer alerts "as soon as" a threat, attack, or suspicious activity was detected within LifeLock's network, enabling customers to prevent identity theft.[126] LifeLock coupled these claims with warnings

---

[122] Ex. 6, FTC-000004-05.
[123] *Id.* at FTC-000008-09.
[124] Ex. 12, FTC-0002086-87.
[125] *See* Ex. 13, Ref. 112 at :54-1:01; File: ZTVT4730h_vanity.mp4 at :52-1:06 (Ref. 114); Ref. 116 at :30-48; ZTVT4991_PL_Original_OPT_W_GIU_Micharger_PL_120_110813_AJ_Desktop.mp4, at :30-:48 (Ref. 117); Ref. 123 at :32-55.
[126] *See e.g.*, Ex. 13, Ref. 106 at 1:06-1:16, Ref. 114 at :52-1:06, Ref. 116 at :36-:48, and Ref. 123 at :32-:55.

that other identity theft protection services notified consumers **too late**.[127] For example, LifeLock told consumers in a late 2012 Holiday advertisement:

> You can't be on the lookout **24/7, but LifeLock can**. They're **relentless** about protecting your identity **every minute of every day**.
>
> When someone tries to **take over your bank accounts, drain the equity in your home**, or even tries to buy a car in your name, **LifeLock is on guard**.
>
> And with **LifeLock's 24/7 alerts** they contact you by text, phone, or email **as soon as** they detect suspicious activity in their network.

(Emphasis supplied.)[128] In November 2013, LifeLock's website said:

> **Our mission is to provide relentless protection for members.**
>
> * * * *
>
> LifeLock is more than just a credit monitoring service. We help protect your personal information using a combination of data surveillance techniques and outstanding member service, **24 hours a day, seven days a weeks, 365 days a year.**
>
> * * * *
>
> LifeLock's monitoring services relentlessly protect your credit and personal information from identity theft and fraud, **24 hours a day, seven days a week, 365 days a year.**

(Emphasis supplied.)[129]

The "proactive alert" services[130] LifeLock touted included "Identity Alerts" that are "sent as soon as LifeLock detects, within its network database, its members' Social Security number, name, address, or date of birth in applications for credit and

---

[127] Ex. 13, Ref. 122 at :49-:57.
[128] Ex. 13, Ref. 106 at :45-1:17.
[129] Ex. 6, at FTC-000006, 000008.
[130] (b)(3):6(f),(b)(4)

Ex. 64, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (Mar. 31, 2014) LIFELOCK-2307-322, 2312-15..

services."[131] LifeLock's Ultimate membership included "Checking and Savings Account Application Alerts"[132] and "Bank Account Takeover Alerts."[133] (Collectively "Bank Account Alerts.") The Ultimate service also included Credit Inquiry Activity Alerts ("Credit Inquiry Alerts") when "inquiries are made" against a member's credit file.[134]

Although LifeLock painted dire consequences from notification delays and trumpeted its 24/7 monitoring and notifications, it did not live up to its promises. In reality, LifeLock never had a system for providing Credit Inquiry Alerts "as soon as" detected, did not provide Bank Account Alerts on weekends, and delayed alerts during planned maintenance activities.

1. LifeLock Systematically Delayed Credit Inquiry Alerts.

While continuing to flood the market with its 24/7 claims, at no point did LifeLock provide Credit Inquiry Alerts "as soon as" its network detected a threat, attack, or suspicious activity.[135] In fact, delays built into LifeLock's system ensured that it could not fulfill its promise.

---

[131] *Id.* at LIFELOCK-2307. LifeLock advertisements noted that its alerts were limited to activities "within its network." *Id.* All of the alert deficiencies discussed herein were within LifeLock's network.

[132] *Id.* LifeLock provides "when the member's personal information is identified in new bank account applications."

[133] *Id.* LifeLock provides when there are "changes to identity data or attempts to add new account holders to existing checking and savings accounts at financial institutions within the LifeLock network."

[134] *Id.*

[135] Ex. 13, Ref. 112 at :49-:57, 114 at :54-1:01, 123 at :32-:55.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

Finally, LifeLock did not then immediately transmit this alert, but in accordance with its own processing cycle, delayed up to another three hours before alerting its members.[138]

2. LifeLock Suppressed Bank Account Alerts on Weekends.

In addition to these systematic delays, from early-November 2012 to early-July 2013 (eight months), LifeLock *elected* not to process Bank Account Alerts on the vast majority of weekends,[139] telling its vendor to "delay the transmission of such alerts to LifeLock over these weekend time periods."[140] For 42 weekends from October 2012 to November 2013, LifeLock members could not receive a notification "as soon as" or

---

[136] Ex. 65, ¶ 7, Declaration of Steve Seoane, Chief Product Officer, LifeLock, Inc., (March 6, 2015) ("Seoane Decl."). The three credit bureaus are TransUnion, Equifax, and Experian.

[137] *Id.* It is unclear from Mr. Seoane's Declaration how long (1 hour, 6 hours, 12 hours) it takes for CSID to go through the file.

[138] *Id.* at ¶ 8. Not until November 2013 did LifeLock begin processing these alerts as received from CSID. *Id.*

[139] Ex. 67, Letter from Andrew G. Berg, Greenberg Traurig, LLP, to Gregory J. Madden, Federal Trade Commission (July 2, 2014), LIFELOCK-0093533-44 and 0093632-35 (Annex 18).

[140] *Id.* at LIFELOCK-0093539.

"whenever" LifeLock detected a threat in its network.[141] Moreover, a review of the weekend alerts information shows the "weekend" actually ran from Friday evening to Monday morning.[142]

3. LifeLock Did Not Send Alerts During "Planned Maintenance" Activities.

Finally, LifeLock did not provide its promised "24/7" alerts during planned maintenance activities. In fact, LifeLock's own "gaps" analysis identified several periods when it did not send alerts.[143] From October 2012 to March 2014, there were 141 "planned maintenance" periods of at least five hours when LifeLock failed to send Identity Alerts or Bank Account alerts.[144] Among these, LifeLock did not send Identity Alerts for five hours or more 46 times, and Bank Account Alerts for five hours or more 95 times.[145] This is particularly egregious because LifeLock used the supposed 24/7 immediacy of its alerts to distinguish its services from its competitors.[146]

III. DISCUSSION

A. LifeLock Violated the Order.

This Court has the inherent authority to enforce its Order through civil contempt.[147] The FTC has the burden of showing by clear and convincing evidence that

---

[141] *See id.*; Ex. 32, Miles Decl. ¶¶ 5, 10.
[142] *Id.*, Ex. 67, Annex 18, LIFELOCK-0093632-35; Ex. 32, Miles Decl. ¶¶ 5, 10.
[143] Ex. 32, Data Decl. ¶¶ 4-12.
[144] *Id.* at Ex. C.
[145] *See id.* at Ex. B.
[146] Ex. 13, Ref. 122 at :49-1:11.
[147] *Shillitani v. United States*, 384 U.S. 364, 370, 86 S. Ct. 1531, 1535, 16 L. Ed. 2d 622 (1966).

LifeLock knew of, and violated, a specific and definite order of the Court.[148] Because there is clear and convincing evidence that LifeLock violated specific and definite provisions of the Order they negotiated and signed in four ways, LifeLock is in contempt.[149]

1. LifeLock Violated the Order's Information Security Provision.

The Order requires LifeLock to "establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." Section II. The Order requires that its information security program be appropriate in light of "the nature and scope of the entity's activities" and "the sensitivity of the [consumer's] personal information collected." *Id.* Additionally, the program, its content, and implementation "must be fully documented in writing." *Id.*

LifeLock maintains consumers' most sensitive personal information, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) Thus, it is not surprising that LifeLock's own documents state that its protection of highly sensitive personal information should be at, or above, that for businesses collecting personal information as a corollary to their main business.[150] Specifically, LifeLock's own security assessment explains:

> LifeLock's product is the protection of a consumer's identity. A fundamental component of the protection is that LifeLock itself not be the source of information that would enable the compromise of a member's identity.

---

[148] *FTC v. Affordable Media, LLC*, 179 F.3d 1228, 1239 (9th Cir. 1999).
[149] *See id.*
[150] Ex. 62, at LIFELOCK-0133868.

> Therefore, the focus of LifeLock's operation is to protect the member's sensitive PII **to a greater level** that [sic] would be done by other companies that have collected such information as a byproduct of their business.

(Emphasis supplied.)[151]

In fact, LifeLock's program was woefully deficient in basic security functions – security patch/software update management, responding to identified vulnerabilities, securely managing production systems changes, and conducting and managing all necessary scanning and monitoring activities.

Not surprisingly, these failures were glaringly apparent to LifeLock information security employees. In September 2012, two and a half years *after* entry of the Order against LifeLock for having inadequate information security, LifeLock's Director of Information Security told its CIO that LifeLock was only covering 20% of its production systems with automated scans and "**our current coverage for discovering system vulnerabilities before the bad guys is not adequate**."[152] (Emphasis supplied.)

A September 2012 third party due diligence audit discovered issues that LifeLock was completely unaware of because the audit was of "areas we have not yet inspected ourselves."[153] In January 2013, LifeLock's information security consultant told its Internal Auditor that penetration test findings from September 2012 had not been addressed and "[p]en tests were in September – hello, its January of the following

---

[151] *Id.*

[152] Ex. 58, at LIFELOCK-0089026.

[153] *Id.* As a result, the email requested three additional full time employees for the upcoming year. *Id.* at LIFELOCK-0089027.

year."[154] In February 2013, the Internal Auditor reported to the Board of Directors Audit Committee that LifeLock's top ranked risk was IT Enterprise Security.[155] LifeLock's own risk assessment scored this risk as "high as controls are not consistently followed or are not in place."[156] Across all the areas assessed - Financial, Operational, Compliance, Strategic, Information Technology - Enterprise Security was the highest risk due to risks from "[l]ack of overall security strategy for compliance, access management issues, no threat analysis, no configuration standards."[157] IT Applications/Databases tied for the second highest risk. The Internal Auditor described this risk as "[n]o change management, no patch management, poor data quality or integrity, access management issues."[158]

Importantly, LifeLock knew it was failing to provide critical security patches within the 30 days of their release required by PCI DSS. Yet this failure persisted for months. In September 2012, (b)(3):6 (f),(b) reported to LifeLock that it was missing 94 important/critical patches.[159] In December 2012, a risk assessment sent to LifeLock's Internal Auditor states that "P & T staff and management need to take vulnerability and patch management more seriously and ensure that VRR's are submitted and worked to remediate vulnerabilities to get the numbers down to an acceptable level."[160] Three months later, LifeLock's information security consultant told senior LifeLock managers

[154] Ex. 30, at LIFELOCK-0038509.
[155] Ex. 68, at LIFELOCK-0051795-10.
[156] Ex. 14, at LIFELOCK-0051793-002.
[157] *Id.*
[158] *Id.*
[159] Ex. 28, at LIFELOCK-2147, 2174-76.
[160] Ex. 69, LIFELOCK-0084028-003.

that Windows and Linux system patching was behind by at least 3 months and was thus well outside the 30 day PCI DSS requirement for remediating high vulnerabilities and outside the 60 and 90 day requirements for medium and low vulnerabilities.[161] Predictably, in June 2013, the PCI assessor noted that on the server he examined, a missing "Critical" patch had not been applied for months, and that no patches had been applied at all for many months.[162] The reason LifeLock identified for this critical failure was "resources" and priorities.[163]

An analysis of LifeLock's patching information, such as it was, confirms LifeLock's patching did not meet PCI-mandated timeframes – *i.e.*, 56.6% of critical Microsoft patches were not applied within 30 days and 48% of non-critical patches were not applied within 90 days.[164] Obviously, this does not even approach the two week timeframe used by financial institutions that hold such sensitive personal information.

This problem was compounded because LifeLock improperly downgraded risks and untimely applied patches. Specifically, LifeLock unilaterally downgraded vendor patch ratings without documentation, masking critical vulnerabilities as low priorities.[165] In April 2013, their PCI assessor discovered this practice and demanded it stop.[166] However, LifeLock did not require documentation until July 2013.[167]

---

[161] Ex. 31, at LIFELOCK-0019638.
[162] Ex. 24, at LIFELOCK-39705.
[163] *Id.*
[164] Ex. 20, Cole Rpt. ¶¶ 102 and 104.
[165] Ex. 22, at LIFELOCK-0038588; *see* Ex. 73, Balasubramanian Decl. ¶ 39.
[166] *See* Ex. 24, at LIFELOCK-0039705. *See also* Ex. 25, at LIFELOCK-0009260 (noting "[p]atch classification downgraded without documented justification.")
[167] Ex. 26, at LIFELOCK-0053865.

Implementing a process documenting downgrading apparently yielded 83 critical and high VRRs after months with only two.[168]

Similarly, an analysis of LifeLock's VRR logs establish it did not timely discover, remediate, or document identified vulnerabilities regardless of categorization as critical, high, medium, or low. For example, 60.5% of LifeLock's self-reported critical VRRs were not resolved in 30 days and over 36.4% were not resolved for over 90 days.[169] Considering the sensitive personal information LifeLock held, this is well beyond the 15 days that it should have taken LifeLock to resolve these vulnerabilities if it was operating at the level of a financial institution.[170]

Importantly, but not surprisingly given LifeLock's vulnerability remediation management system, LifeLock did not even look at the vast majority of VRRs from the late-2012 penetration tests for months.[171] In fact, LifeLock ignored the highest severity vulnerabilities (missing anti-virus, directory traversal, guessable manager passwords, and reusing local administrator passwords) from its own auditors, (b)(3):6(f), (b)(4) and (b)(3):6 (f),(b)(4) until March 2013, leaving LifeLock's system and consumers' information vulnerable.[172]

Moreover, LifeLock lost, found, and lost again multiple high priority penetration test vulnerabilities, and they remained unresolved for over a year. For example, LifeLock lost track of six of the vulnerabilities identified in late 2012 penetration tests

---

[168] Ex. 73, Balasubramanian Decl. ¶ 43.
[169] Ex. 20, Cole Rpt. ¶ 88.
[170] *Id.* at ¶ 170.
[171] *Id.* at ¶ 72.
[172] *See discussion supra at* pp. 18-20.

until July 2013,[173] then erroneously reported five FishNet vulnerabilities as "corrected and retested" in the 2013 PCI report.[174] In October 2013, LifeLock again identified five (b)(3):6(f), (b)(4) and one (b)(3):6 (f),(b)(4 vulnerability as unresolved.[175] Unbelievably, a number of these vulnerabilities remained unresolved into August 2014. In fact, in August 2014, LifeLock confessed that four penetration test VRRs were closed "without documentation of evaluation."[176] As late as January 2014, LifeLock's process for managing VRRs was unclear.[177] In August 2014, LifeLock still had 322 VRRs that had been open over 150 days, 138 of them ranked Critical or High.[178]

A central element of an effective information security program is managing system changes so systems remain secure. But LifeLock failed to implement a change management system.[179] LifeLock's third party penetration tester highlighted its failures in November 2012.[180] Its information security consultant again highlighted the same failure in March 2013.[181] LifeLock's PCI assessor did so yet again in May 2013.[182] An on-site information security consultant highlighted the problem once again in July

---

[173] Ex. 37, at LIFELOCK-0025172, 0025172.
[174] Ex. 3, at 0097204-05; Ex. 20, Cole Rpt. ¶¶ 64-72.
[175] *See* Ex. 38, at LIFELOCK-008194950, 0081954.
[176] Ex. 40, at LIFELOCK-0110774-75. As of the September 19, 2014 response, three of these were "reopened" and awaiting resolution. *Id.*
[177] Ex. 49, LIFELOCK-0033450-452.
[178] Ex. 50, LIFELOCK-0134378-85.
[179] Ex. 20, Cole Rpt. ¶¶ 128-34.
[180] Ex. 29, at LIFELOCK-0053409.
[181] Ex. 52, LIFELOCK-0026183.
[182] Ex.16, at LIFELOCK-0095896.

2013.[183] Despite these warnings, LifeLock failed to develop and approve a new Change Management Standard until February 2014.[184]

Finally, LifeLock failed to run PCI-required vulnerability scans on all of its virtual network within its PCI environment.[185] Ensuring that systems are secure requires scanning all of the servers in the PCI environment.[186] This is particularly important because vulnerabilities on one server can lead to access to other servers.[187] Although PCI DSS requires quarterly scans, LifeLock first scanned two of its VLANs after three quarters had already passed. Thus, unbelievably, LifeLock had operated in the PCI environment for nine months without any scanning.[188]

Using a number of these deficiencies a ransomware attacker successfully compromised LifeLock's system (e.g., outdated and unpatched software, flawed daily scanning). Simply put, for *years* after entry of the Order, LifeLock failed to "establish, implement and thereafter maintain" anything remotely close to an appropriate information security program pursuant to the Order.

2. LifeLock Misrepresented Its Protection of Consumers' Personal Information.

This Court's Order enjoins LifeLock from "misrepresenting in any manner, expressly or by implication, the manner or extent to which they maintain and protect the privacy, confidentiality, or security of any personal information collected from or about

[183] Ex. 53, LIFELOCK-0029627.
[184] Ex. 54, LIFELOCK-0033420-23.
[185] Ex. 40, at LIFELOCK-0110780.
[186] Ex. 20, Cole Rpt. ¶¶ 50 and 153.
[187] *Id.*
[188] Ex. 40, LIFELOCK-0110780.

consumers." Section I.B.[189] A central component of LifeLock's identity theft protection service is securing its customers' highly sensitive personal information.

In a ubiquitous commercial featuring Montel Williams, LifeLock's CEO Todd Davis claimed "we meet the high levels of security data handling, PCI Level 1."[190] LifeLock claimed tens of thousands of times in commercials and constantly on its website that it "meets" PCI standards. LifeLock's CEO further claimed LifeLock secured consumers' sensitive information to the level of "your financial institution."[191] LifeLock drove home their claims that it protected consumers' sensitive information at that highest level by telling consumers it protected consumers' information "relentlessly," "no one" protected them better, it would "Protect Your Identity," and it provided the most "comprehensive identity theft protection."[192]

Yet LifeLock delivered nowhere near its promises while making these claims. First, contrary to its promises, because of the failures detailed above (patch management, vulnerability management, change management, PCI scanning), LifeLock's protection did not continuously meet PCI requirements. To pass PCI DSS, LifeLock falsely claimed it "corrected and retested" penetration test vulnerabilities. In fact, LifeLock's own records show some of these vulnerabilities were not addressed for months after it "passed" its 2013 PCI certification.[193] This fact is further demonstrated by the May 2013 PCI compliance gap analysis confirming that for 6 of the 12 PCI DSS

---

[189] Ex. 1.
[190] *See supra* footnote 4.
[191] *Id.*
[192] *See supra*, footnotes 13-17.
[193] Ex. 40, at LIFELOCK-110774-75; *see supra* footnote 63.

requirements LifeLock was not fully PCI compliant.[194] Perhaps most damning, LifeLock failed to apply critical patches in the PCI-mandated time period of 30 days.[195] A failure noted by two of LifeLock's information security consultants on separate occasions and confirmed by its own patching records.[196] Even if LifeLock had met PCI standards at one point, which it did not, it plainly did not *meet* them on an ongoing basis as CEO Davis and LifeLock's website claimed.

LifeLock also falsely claimed it protected consumers' information like financial institutions, and better than anyone else. In reality, LifeLock's information security program did not even meet minimum information security standards, so it certainly was not the information security expected of financial institutions nor did it protect consumers' information better than anyone else.[197]

3. LifeLock Also Misrepresented Its Identify Theft Protection Services.

The Order prohibits LifeLock from misrepresenting in any manner, expressly or by implication "the means, methods, procedures, effects, effectiveness, coverage, or scope of such product, service, or program." Section I.A.5. LifeLock represented that it "relentlessly" protected members' identity by continually monitoring its network on a 24/7 basis to protect its members "every minute of every day."[198] Its advertisements claimed consumers would get alerts "as soon as" or "whenever" a threat, attack, or

---

[194] Ex. 16, at LIFELOCK-0095895.
[195] Ex. 20, Cole Rpt. ¶¶ 105-08.
[196] Ex. 47, at LIFELOCK-0085248; Ex. 31, at LIFELOCK-0019638; Ex. 20, Cole Rpt. ¶¶ 105-08.
[197] Ex. 20, Cole Rpt.¶¶ 169-70.
[198] *See supra* footnotes 122-29.

suspicious activity was detected within LifeLock's network.[199] LifeLock coupled these claims with warnings that others' services notified consumers too late.[200] These misrepresentations violated Section I.A.5 for three reasons.

First, LifeLock did not provide members Credit Inquiry Alerts "as soon as" or "whenever" activity was detected in its network, but rather suspicious activity detected in LifeLock's network could have been delayed for almost 24 hours (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) and then delayed again (b)(3):6(f),(b)(4) before it got to LifeLock.[201] Prior to November 2013, LifeLock then delayed up to 3 additional hours before notifying customers.[202] To this day, Credit Inquiry Alerts are not provided as soon as a member's information is detected in LifeLock's network, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4)

Second, every weekend from November 2-3, 2012 to July 6-7, 2013, (42 weekends) LifeLock delayed processing Bank Account Alerts, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) over these weekend time periods."[203] All the while, LifeLock's advertisements did not tell its premium-paying Ultimate customers that the service did not include weekends.

---

[199] *See e.g.*., Ex. 13, Ref. 106 at 1:06-1:16, 114 at :52-1:06, 116 at :36-:48, and 123 at :32-:55; Ex. 6, at FTC-000004-05.
[200] Ex. 13, *see e.g.*, Ex. 13, Ref. 122 at :49-1:11.
[201] *See* Ex. 65, Seoane Decl. ¶¶ 7-8.
[202] During April-November 2013 there was up to a 3-hour gap from receipt to processing. Prior to March 2013, LifeLock did identify when it processed these alerts after receipt. Ex. 64, at LIFELOCK-2315-16.
[203] Ex. 67, at LIFELOCK-0093539.

Lastly, from at least October 2012 through March 2014, LifeLock did not send alerts during planned system maintenances. On at least 141 occasions from October 2012 through March 2014, those outages lasted 5 hours or more.[204] LifeLock never disclosed this fact to its customers, all the while claiming consumers should purchase its service because unlike competitors LifeLock notified consumers as soon as it detected a threat in its network.

4. LifeLock Violated the Order's Recordkeeping Requirements.

Section VIII of the Order requires LifeLock to create and retain all documents necessary to demonstrate full compliance with the Order. Section VIII.A.7. Proper log storage and archiving, and the ability to review them and re-create events, are necessary and critical parts of a comprehensive information security program.[205] Without documentation, a company cannot know its own security status.[206] LifeLock did not even come close to retaining all documents necessary to show Order compliance. For example, LifeLock did not retain and was unable to recreate the daily logs generated by (b)(3):6(f), (b)(4) its Security Incident and Event Management tool. Significantly, LifeLock does not have records reflecting the patch histories for the over 550 servers it has decommissioned.[207] LifeLock is also unable to identify when those

[204] Ex. 32, Miles Decl. ¶ 11, Ex. C.
[205] Ex. 20, Cole Rpt. ¶¶ 54, 97, 141-43, and 147.
[206] *Id.* at ¶ 141.
[207] *See* Ex. 56, at FTC-0002172-73.

servers were decommissioned.[208] LifeLock's recordkeeping failures therefore violate the Order.

B. Consumers Are Entitled to Redress

Civil contempt sanctions can either coerce the defendant into compliance or compensate victims for losses sustained by the contempt.[209] If consumers suffer losses, compensation is the appropriate remedy.[210] Compensatory damages in civil contempt are based on actual loss[211] and injured consumers are entitled to full remedial relief.[212] Civil contempt damages need only be proven by a preponderance of the evidence.[213]

In an FTC enforcement action (in either a contempt motion or in a new case[214]), the fraud occurs at the time of the selling.[215] The Ninth Circuit found that injury in an

---

[208] *Id.* LifeLock became aware of the FTC's investigation in December 2013 and on March 13, 2014, the FTC first requested information and notified LifeLock of its obligation to suspend document destruction procedures and take other measures to prevent destruction of documents relevant to the investigation. Ex. 72, FTC Letter from Gregory Madden, Federal Trade Commission, to Andrew Berg, Greenberg Traurig, LLP, (March 13, 2014) FTC-0002196-2201, FTC-0002200.

[209] *United States v. United Mine Workers*, 330 U.S. 258, 303-04, 67 S. Ct. 677, 701, 91 L. Ed. 884 (1947); *Ahearn ex rel. NLRB v. Int'l Longshore & Warehouse Union, Locals 31 & 24*, 721 F.3d 1122, 1131 (9th Cir. 2013); *see also McGregor v. Chierico*, 206 F.3d 1378, 1385 n.5 (11th Cir. 2000) (FTC contempt action).

[210] *See FTC v. EDebitPay, LLC*, 695 F.3d 938, 945 (9th Cir. 2012); *McGregor*, 206 F.3d 1378, 1387-89 (11th Cir. 2000).

[211] *United Mine Workers*, 330 U.S. at 303-04.

[212] *McComb v. Jacksonville Paper Co.*, 336 U.S. 187, 193, 69 S. Ct. 497, 500, 93 L. Ed. 599 (1949).

[213] *See FTC v. Kuykendall*, 371 F.3d 745, 767 (10th Cir. 2004) (*en banc*); *McGregor*, 206 F.3d at 1387. *Ahearn*, 721 F.3d at 1129 (noting every circuit to consider the issue has adopted the preponderance standard).

[214] *FTC v. Figgie Int'l*, 994 F.2d 595, 605-06 (9th Cir. 1993); *FTC v. BlueHippo Funding, LLC*, 762 F.3d 238, 244-45 (2d Cir. 2014)

[215] *See Figgie Int'l*, 994 F.2d at 606; *BlueHippo Funding*, 762 F.3d at 244 (in FTC contempt cases, "the injury occurs at the moment the seller makes those

FTC matter is not the diminution of value in the thing sold, but rather the fact that consumers purchased goods or services based on material misrepresentations.[216] Therefore, once the FTC proves defendants have made a widespread, material misrepresentation, each consumer's reliance on those misrepresentations is presumed and damages, therefore, are presumed to be defendants' gross revenues.[217] The burden then shifts to the defendants to prove with particularity that individual consumers did not rely on defendants' misrepresentations.[218] Here, LifeLock's information security and alerting claims were widely disseminated through extensive television advertising and LifeLock's website. They were both express and related to a central characteristic of LifeLock's service and are thus presumed material for both reasons.[219] As detailed above, these information security and alerting claims were misrepresentations.

LifeLock members, therefore, are presumed to have relied on such widely disseminated misrepresentations and are entitled to full redress.[220] LifeLock did not deliver what it promised, and thus, customers did not get what they paid for. LifeLock

---

misrepresentations"); *Kuykendall*, 371 F.3d at 766 (citing *Figgie* in rejecting argument that value of magazines consumers actually received should offset customer's recovery).

[216] *Kuykendall*, 371 F.3d at 766 (citing Figgie in rejecting the argument that the value of magazines consumers actually received should offset consumers' recovery).

[217] *BlueHippo Funding*, 762 F.3d at 245 (quoting *McGregor*, 206 F.3d at 1388).

[218] *See Kuykendall*, 371 F.3d at 766-67 ("[T]he defendants may put forth evidence showing offset because *certain consumers* . . . were satisfied with their purchases.") (Emphasis supplied).

[219] *FTC v. Pantron I Corp.*,33 F.3d 1088, 1095-96 (9th Cir. 1994); *In the Matter of Thompson Medical Co.*, 104 F.T.C. 648, 1984 FTC LEXIS 6, at *375 (November 23, 1984) *aff'd Thompson Medical Co., Inc. v. FTC*, 791 F.2d 189 (D.C. Cir. 1986).

[220] *Figgie Int'l*, 994 F.2d at 605-06 ("A presumption of actual reliance arises once the [FTC] has proved that the defendant made material misrepresentations, that they were widely disseminated, and that consumers purchased the defendant's product.").

is thus liable for the hundreds of millions of dollars consumers spent in monthly payments for those undelivered services, unless it can rebut that presumption by proving that particular customers did not rely on its false claims.[221]

IV. CONCLUSION

For the foregoing reasons, the Court should grant the FTC's request for a Contempt Order against LifeLock.

Respectfully submitted,

Dated: July 21, 2015

s/ Gregory J. Madden
GREGORY J. MADDEN
SUSAN H. POPE
HONG PARK
Federal Trade Commission
Division of Enforcement
Mailcode: CC-9528
600 Pennsylvania Ave., NW
Washington, DC 20580
(202) 326-2426, gmadden@ftc.gov
(202) 326-3302, spope@ftc.gov
(202) 326-2158, hpark@ftc.gov
(202) 326-3197 (facsimile)

Attorneys for Plaintiff
Federal Trade Commission

[221] *Kuykendall*, 371 F.3d at 766-67; *see also FTC v. Bronson Partners, LLC*, 654 F.3d 359, 369 (2d Cir. 2011); *BlueHippo Funding, LLC*, 762 F.3d at 244 and 245 (quoting *McGregor*, 206 F.3d at 1388).

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

APPENDIX TO EXPERT REPORT OF DR. ERIC B. COLE
(Index of Documents Considered; Index of Documents Cited)

***This Appendix contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

INDEX OF DOCUMENTS CONSIDERED
EXPERT REPORT OF DR. ERIC B. COLE

Bates Numbers	Document Description
LIFELOCK-1007-2227	*Attestation of Compliance for Onsite Assessments – Merchants- Version 2.0*, Payment Card Industry Security Standards Council (Oct. 2010)
LIFELOCK-3122-48	*Penetration Test Report for id:analytics*, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) (Mar. 21, 2014)
LIFELOCK-3166-74 (2014 04 15 FTC Response (Specs 3 11-23 27-28 31))	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Attorney, Federal Trade Commission (Apr. 15, 2014)
LIFELOCK-3288-94	*Penetration Testing Scope and Rules of Engagement for id:analytics*, (b)(3):6(f),(b)(4) (Nov. 25, 2013)
LIFELOCK-9205	Email from Gwen Ceylon to Jenner Holden and Tony Valentine (Oct. 15, 2012)
LIFELOCK-9206-08	LifeLock PCI Environment Diagram (Oct. 9, 2012)
LIFELOCK-9209-11	LifeLock PCI Environment Diagram (Oct. 9, 2012)
LIFELOCK-9283	*LifeLock Inc. 2013 PCI Audit*, (b)(3):6(f),(b)(4) Virus Updates and Patching Screen Shot, from C. Ebright, Senior Windows Engineer (Apr. 10, 2013)
LIFELOCK-9620	Feb 2012 PCI Scan.csv
LIFELOCK-9621	*Untitled Spreadsheet*
LIFELOCK-9622	*Untitled Spreadsheet*
LIFELOCK-9623	*Feb 2012 PCI Scan.csv*
LIFELOCK-9624	*Feb 2012 PCI Scan.csv*
LIFELOCK-9625	*Feb 2012 PCI Scan.csv*
LIFELOCK-9626	*Feb 2012 PCI Scan.csv*
LIFELOCK-9656	Questions on 2012 Pen Test
LIFELOCK-0010010 (VRR 81560)	Email from (b)(3):6(f),(b)(4) to Austin Appel (May 15, 2013)
LIFELOCK-0010126	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Sep. 19, 2013)
LIFELOCK-0010181-83	Email from (b)(3):6(f),(b)(4) to Rich Stebbins, (b)(3):6(f),(b)(4 (b)(3):6(f),(b)(4) and David Bridgman (Mar. 18, 2013)
LIFELOCK-0010210	Email from (b)(3):6(f),(b)(4) to David Bridgman, AnneMarie Olson and Austin Appel (May 30, 2013)
LIFELOCK-0010316-17	Email from (b)(3):6(f),(b)(4) to Jim Casselbury (Sep. 19, 2013)
LIFELOCK-010423-24	Email from (b)(3):6(f),(b)(4) to Austin Appel (Sep. 19, 2013)

LIFELOCK-0010675-76	Email from AnneMarie Olson to (b)(3):6(f),(b)(4) and David Bridgman (Mar. 13, 2013)
LIFELOCK-0011678-79	Email from (b)(3):6(f),(b)(4) to Rich Stebbins, (b)(3):6(f),(b)(4) Renee Ramirez, and (b)(3):6(f),(b)(4) (Mar. 8, 2013)
LIFELOCK-0011693	Email from (b)(3):6(f),(b)(4) to Richard Dear and Ian Conrad (Feb. 25, 2013)
LIFELOCK-0012099-100	Email from (b)(3):6(f),(b)(4) to Austin Appel, (Jun. 6, 2013)
LIFELOCK-0012264-65	Email from (b)(3):6(f),(b)(4) to Austin Appel (Dec. 2, 2013)
LIFELOCK-0012287-88	Email from (b)(3):6(f),(b)(4) to (b)(3):6(f),(b)(4) (Mar. 6, 2013)
LIFELOCK-0013100-06	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Aug. 23, 2013)
LIFELOCK-0013254-55	Email from (b)(3):6(f),(b)(4) to David Bridgman, (b)(3):6(f),(b)(4) and Austin Appel (Feb. 20, 2013)
LIFELOCK-0013367	Email from AnneMarie Olson to (b)(3):6(f),(b)(4) (Jun. 20, 2013)
LIFELOCK-0018740-42	Email from (b)(3):6(f),(b)(4) to Austin Appel (Oct. 7, 2013)
LIFELOCK-0019331-41	Email from (b)(3):6(f),(b)(4) LifeLock, to (b)(3):6(f),(b)(4) Brian Kao, (b)(3):6(f),(b)(4), and (b)(3):6(f),(b)(4) (Jul. 16, 2013)
LIFELOCK-0021289-94	Email from (b)(3):6(f),(b)(4) to (b)(3):6(f),(b)(4) (Jul. 9, 2013)
LIFELOCK-0021374-76	Email from (b)(3):6(f),(b)(4) to Michael Hoffman (Dec. 17, 2013)
LIFELOCK-0021380-81	Email from (b)(3):6(f),(b)(4) to Rich Stebbins, (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4), Renee Ramirez, and (b)(3):6(f),(b)(4) (Mar. 7, 2013)
LIFELOCK-0022184-88	Email from (b)(3):6(f),(b)(4) to Michael Hoffman (Dec. 13, 2013)
LIFELOCK-0022345	*Feb 2012 PCI Scan.csv*
LIFELOCK-0022953-55	Email from (b)(3):6(f),(b)(4) to Andrew Citro (Feb. 14, 2014)
LIFELOCK-0023364-65	Email from (b)(3):6(f),(b)(4) to (b)(3):6(f),(b)(4) (Mar. 6, 2013)
LIFELOCK-0025172-74	Email from (b)(3):6(f),(b)(4) and Brian Kao (Jul. 16, 2013)
LIFELOCK-0025175	LifeLock Excel Spreadsheet.
LIFELOCK-0025839-	Email from (b)(3):6(f),(b)(4) to Michael Hoffman (Dec. 23,

41	2013)
LIFELOCK-0026924-25	Email from (b)(3):6(f),(b)(4) to Austin Appel (May 15, 2013)
LIFELOCK-0027588-89	Email from (b)(3):6(f),(b)(4) to Austin Appel (Sep. 16, 2013)
LIFELOCK-0028073-74	Email from AnneMarie Olson to (b)(3):6(f),(b)(4) (Mar. 6, 2013)
LIFELOCK-0029301-02	Email from (b)(3):6(f),(b)(4) to Michael Hoffman (Mar. 7, 2014)
LIFELOCK-0030131-32	Email from (b)(3):6(f),(b)(4) to Austin Appel (Jun. 6, 2013)
LIFELOCK-0031169-78	Email from (b)(3):6(f),(b)(4) to Tony Valentine (Jul. 15, 2013)
LIFELOCK-0031556-57	Email from (b)(3):6(f),(b)(4) to Michael Hoffman (Dec. 13, 2013)
LIFELOCK-0032746	Email from Austin Appel to (b)(3):6(f),(b)(4) (May 22, 2013)
LIFELOCK-0032819-20	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Jul. 31, 2013)
LIFELOCK-0033420-23	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson (Feb. 11, 2014)
LIFELOCK-0033464	Email from (b)(3):6(f),(b)(4) to David Bridgman, AnneMarie Olson, and Austin Appel (May 30, 2013)
LIFELOCK-0033479	Email from (b)(3):6(f),(b)(4) to David Bridgman and Austin Appel (Mar. 25, 2013)
LIFELOCK-0033484-85	Email from (b)(3):6(f),(b)(4) to David Bridgman and Austin Appel (Mar. 26, 2013)
LIFELOCK-0033553	Email from (b)(3):6(f),(b)(4) to David Bridgman, AnneMarie Olson, and Austin Appel (May 30, 2013)
LIFELOCK-0033573-74	Email from (b)(3):6(f),(b)(4) to Austin Appel (Jul. 19, 2013)
LIFELOCK-0033623	Email from (b)(3):6(f),(b)(4) to Austin Appel (Mar. 26, 2013)
LIFELOCK-0033667-68	Email from (b)(3):6(f),(b)(4) to Austin Appel (Aug. 7, 2013)
LIFELOCK-0033696-97	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Jul. 31, 2013)
LIFELOCK-0033749	Email from (b)(3):6(f),(b)(4) to Austin Appel (Apr. 3, 2013)
LIFELOCK-0033753-54	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Jul. 31, 2013)
LIFELOCK-0033787-88	Email from (b)(3):6(f),(b)(4) to David Bridgman, AnneMarie Olson, and Austin Appel (May 30, 2013)
LIFELOCK-0033792-93	Email from (b)(3):6(f),(b)(4) to Austin Appel (Aug. 7, 2013)

LIFELOCK-0033853	Email from (b)(3):6(f),(b)(4) to David Bridgman, (b)(3):6(f),(b)(4) and Austin Appel (Mar. 1, 2013)
LIFELOCK-0033888-89	Email from (b)(3):6(f),(b)(4) to Austin Appel (Aug. 7, 2013)
LIFELOCK-0033901-02	Email from (b)(3):6(f),(b)(4) to Austin Appel (Aug. 7, 2013)
LIFELOCK-0033903	Email from (b)(3):6(f),(b)(4) to David Bridgman, (b)(3):6(f),(b)(4) and Austin Appel (Feb. 28, 2013)
LIFELOCK-0034009-10	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Jul. 31, 2013)
LIFELOCK-0034015	Email from (b)(3):6(f),(b)(4) to David Bridgman, AnneMarie Olson, and Austin Appel (May 30, 2013)
LIFELOCK-0034337-42	Email from AnneMarie Olson to (b)(3):6(f),(b)(4) Nathan Shimek, Manager, and (b)(3):6(f),(b)(4) (Jan. 6, 2014)
LIFELOCK-0034364	Email from (b)(3):6 (f),(b)(4) Hatch to AnneMarie Olson (Feb. 27, 2014)
LIFELOCK-0034365-66	LifeLock Security Exception Risk Assessment Form. Submitted by Andrew Citro (Oct. 14, 2013)
LIFELOCK-0034400-01	LifeLock Security Exception Risk Assessment Form. Submitted by Andrew Citro (Oct. 14, 2013)
LIFELOCK-0035991-93	Email from Chris Ebright to (b)(3):6(f),(b)(4) (Apr. 3, 2013)
LIFELOCK-0037156-58	Email from Patrick Serano to Kyle Corupe (Apr. 3, 2013)
LIFELOCK-0037234-37	Email from David Bridgman to (b)(3):6(f),(b)(4) (Apr. 3, 2013)
LIFELOCK-0037541	Email from (b)(3):6(f),(b)(4) to David Bridgman (Mar. 29, 2013)
LIFELOCK-0037568-69	Email from (b)(3):6(f),(b)(4) to David Bridgman (Mar. 29, 2013)
LIFELOCK-0037592-93	Email from (b)(3):6(f),(b)(4) to David Bridgman (Apr. 2, 2013)
LIFELOCK-0037772-75	Email from Jenner Holden to Austin Appel (Nov. 21, 2012)
LIFELOCK-0037992-93	Email from (b)(3):6(f),(b)(4) to Austin Appel (Oct. 29, 2012)
LIFELOCK-0038586-87 (Gwen VRR 81561)	Email from Gwen Ceylon to Tony Valentine (Jan. 7, 2013)
LIFELOCK-0038588-89	Email from Gwen Ceylon to Tony Valentine (Jan. 7, 2013)
LIFELOCK-0038608-10	Email from Gwen Ceylon to Ly Sauer and Nola Isla (Jan. 10, 2013)

LIFELOCK-0038617	Email from Gwen Ceylon to David Bridgman and Tony Valentine (Jan. 11, 2013)
LIFELOCK-0043729-82	LifeLock Information Security Management System Policy. Version 10.0.
LIFELOCK-0051793	LifeLock Excel Spreadsheet. Risk Assessment Detail
LIFELOCK-0051794	LifeLock Excel Spreadsheet. Risk Assessment Detail
LIFELOCK-0051795	LifeLock PowerPoint Presentation. 2013 Internal Audit Plan (Feb. 21, 2013)
LIFELOCK-0074378-477	Payment Card Industry Technical Report. (b)(3):6(f),(b)(4) PCI (May 28, 2013)
LIFELOCK-0074478-487	Payment Card Industry Executive Report. (b)(3):6(f),(b)(4) PCI (May 28, 2013)
LIFELOCK-0075439	LifeLock Excel Spreadsheet. 2013 Risk Assessment Report (Apr. 15, 2013)
LIFELOCK-0075654-56	Email from Austin Appel to (b)(3):6(f),(b)(4) (Jun. 13, 2013)
LIFELOCK-0075657	Screen Shot, Asset Properties and Vulnerability Listing for (b)(3):6(f),(b)(4)
LIFELOCK-0075658	*Untitled Document*
LIFELOCK-0075659	*Untitled Document*
LIFELOCK-0075660	*Untitled Document*
LIFELOCK-0075661	*Untitled Document*
LIFELOCK-0075662	*Untitled Document*
LIFELOCK-0076006-07	Email from David Bridgman to (b)(3):6(f),(b)(4) (Jul. 16, 2013)
LIFELOCK-0076008-09	*LifeLock September 2012 Penetration Test* (Oct. 2012)
LIFELOCK-0076010-11	*LifeLock November 2012 Network Penetration Test* (Nov. 2012)
LIFELOCK-0076572	Email from David Bridgman to (b)(3):6(f),(b)(4) and Austin Appel (Feb. 20, 2013)
LIFELOCK-0076573-74	Payment Card Industry Technical Report. (b)(3):6(f),(b)(4) PCI (Feb. 20, 2013)
LIFELOCK-0079535-36	Email from (b)(3):6(f),(b)(4) to Rich Stebbins and (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) (Jun. 17, 2013)
LIFELOCK-0081942-48	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson (Oct. 21, 2013)
LIFELOCK-0083952	Email from Gwen Ceylon to Jenner Holden, Austin Appel, and David Bridgman (Nov. 27, 2012)
LIFELOCK-0083953-58	*Patch and Vulnerability Management Standard*, Gwen Ceylon
LIFELOCK-0084647	Email from Tony Valentine to (b)(3):6(f),(b)(4) (Feb. 15, 2013)

LIFELOCK-0088601-03	Email from Jenner Holden to Gwen Ceylon and David Bridgman (Dec. 12, 2012)
LIFELOCK-0089117-18	Email from (b)(3):6(f),(b)(4) to Jenner Holden (Dec. 6, 2012)
LIFELOCK-0089119-120	Email from Jenner Holden to (b)(3):6(f),(b)(4) (Dec. 6, 2012)
LIFELOCK-0089185	Email from (b)(3):6(f),(b)(4) to Jenner Holden (Nov. 5, 2012)
LIFELOCK-0089212-13	Email from to Jenner Holden (Nov. 5, 2012)
LIFELOCK-0089220-22	Email from Brian Kao to Jenner Holden and (b)(3):6(f),(b)(4) (Nov. 5, 2012)
LIFELOCK-0089223-24	Email from (b)(3):6(f),(b)(4) to Jenner Holden (Nov. 5, 2012)
LIFELOCK-0089225-26	Email from to Jenner Holden (Nov. 5, 2012)
LIFELOCK-0089227-28	Email from to Jenner Holden (Nov. 5, 2012)
LIFELOCK-0089258	Email from to Jenner Holden (Nov. 12, 2012)
LIFELOCK-0089259-260	Email from to Jenner Holden (Nov. 12, 2012)
LIFELOCK-0089261-62	Email from to Jenner Holden (Nov. 12, 2012)
LIFELOCK-0089263-64	Email from to Jenner Holden (Nov. 12, 2012)
LIFELOCK-0089330-31	Email from to Jenner Holden (Nov. 30, 2012)
LIFELOCK-0092012-14	*Our Financial Estimates*, Deutsche Bank Securities Inc. (Jan. 22, 2014)
LIFELOCK-0110772-81	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Attorney, Federal Trade Commission (Sep. 19, 2014)
LIFELOCK-0132257	Email from (b)(3):6(f),(b)(4) to insosec@lifelock.com (Mar. 11, 2013)
LIFELOCK-0132258	VRR – *Past Due by Group (exclude InfoSec)*, generated by Austin Appel (Mar. 11, 2013)
LIFELOCK-0132298	*VRR – Past Due by Group (exclude InfoSec)*, generated by Austin Appel (Jul. 29, 2013)
LIFELOCK-0132338	*VRR – Past Due by Group (exclude InfoSec)*, generated by Austin Appel (Dec. 23, 2013)
LIFELOCK-0132342	*VRR – Past Due by Group (exclude InfoSec)*, generated by Austin Appel (Jan. 6, 2014)
LIFELOCK-0132350	*VRR – Past Due by Group (exclude InfoSec)*, generated by

	Austin Appel (Feb. 3, 2014)
LIFELOCK-0132478	Letter from Gregory Madden, Attorney, Federal Trade Commission, to Andrew Berg, Counsel to LifeLock, Inc. (Sep. 2, 2014)
LIFELOCK-0132479	*XSS Problem in Jobs Site*
LIFELOCK-0132480	*Vulnerability Fix – Disable AutoComplete*
LIFELOCK-0132481	*Vulnerability Remediation – Cookie Settings*
LIFELOCK-0132482	*Vulnerability Remediation – HTTP Response Information Disclosure*
LIFELOCK-0132483	*Vulnerability Remediation –Hidden Directory Enumeration*
LIFELOCK-0132484	*Vulnerability Remediation – No Clickjacking Protection*
LIFELOCK-0132485	*September 2012 Penetration Test (WWW, Enrollment, & Member Portal)*
LIFELOCK-0132486	*November 2012 Network Penetration Test*
LIFELOCK-0132487	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132488	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132489	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132490	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132491	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132492	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132493	*VRR* REDACTED *) –* (b)(3):6 (f),(b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132494	*VRR* REDACTED *) –* (b)(3):6(f), (b)(4) *community name*, Austin Appel (Oct. 24, 2012)
LIFELOCK-0132495	*VRR (*REDACTED *) – OpenSSL & Apache Updates (low)*, Austin Appel (Oct. 29, 2012)
LIFELOCK-0132496	*VRR (*REDACTED *) – OpenSSL & Apache Updates (low)*, Austin Appel (Oct. 29, 2012)
LIFELOCK-0132497	*Vulnerability Fix – Disable AutoComplete*, Jenner Holden (Nov. 5, 2012)
LIFELOCK-0132498	*Vulnerability Remediation – Fix Caching Directive*, Jenner Holden (Nov. 5, 2012)
LIFELOCK-0132499	*Vulnerability Remediation – Cookie Settings*, Jenner Holden (Nov. 5, 2012)
LIFELOCK-0132500	*Vulnerability Remediation – HTTP Response Information Disclosure*, Jenner Holden (Nov. 5, 2012)

LIFELOCK-0132501	*Vulnerability Remediation – Hidden Directory Enumeration*, Jenner Holden (Nov. 5, 2012)
LIFELOCK-0132502	*Vulnerability Remediation – No Clickjacking Protection*, Jenner Holden (Nov. 5, 2012)
LIFELOCK-0132503	*VRR (*REDACTED[redacted]*) – Directory Traversal*, Jenner Holden (Dec. 6, 2012)
LIFELOCK-0132504	*VRR (*REDACTED[redacted]*) – Directory Traversal*, Jenner Holden (Dec. 6, 2012)
LIFELOCK-0132505	*VRR (Windows Domains) – Local Admin Password*, Jenner Holden (Dec. 6, 2012)
LIFELOCK-0132506	*VRR (Multiple Linux) – Guessable Tomcat Manager Credentials*, Jenner Holden (Dec. 6, 2012)
LIFELOCK-0132507	*VRR (Multiple Linux) – Guessable Tomcat Manager Credentials*, Jenner Holden (Dec. 6, 2012)
LIFELOCK-0132508	*VRR (Multiple Linux) – Guessable Tomcat Manager Credentials*, Jenner Holden (Dec. 6, 2012)
LIFELOCK-0132509	*VRR – (*REDACTED[redacted]*) – Web VPN – No Longer Needed?*, Jenner Holden (Dec. 17, 2012)
LIFELOCK-0132510	*VRR – Check_MK – No Authentication*, Jenner Holden (Dec. 17, 2012)
LIFELOCK-0132511	*VRR – Check_MK – No Authentication*, Jenner Holden (Dec. 17, 2012)
LIFELOCK-0132512	*VRR – (*REDACTED[redacted]*) – SVN Information Disclosure*, Jenner Holden (Dec. 17, 2012)
LIFELOCK-0132513	*VRR –* REDACTED[redacted]*) – SVN Information Disclosure*, Jenner Holden (Dec. 17, 2012)
LIFELOCK-0132514	*Vulnerability Remediation – Hidden Directory Enumeration*, Jenner Holden (Nov. 19, 2012)
LIFELOCK-0132515	*VRR –* REDACTED[redacted] *– Default Credentials*, Jenner Holden (Nov. 12, 2012)
LIFELOCK-0132516	*VRR – (*REDACTED[redacted]*) – Default Credentials*, Jenner Holden (Nov. 12, 2012)
LIFELOCK-0133852-939	*FTC Mandated Independent Assessment of LifeLock Information Security Program.* (b)(3):6(f),(b)(4) (Sep. 23, 2014)
LIFELOCK-0133940-41	*Untitled Document*
LIFELOCK-0133957	*Information Security Procedure: MT_Firedrill, Account Management. Version 1.0*, approved by Jenner Holden (Mar. 21, 2012)
LIFELOCK-0134215-16 (12-9-2014	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Attorney, Federal Trade Commission

Supplemental Response)	(Dec. 9, 2014)
LIFELOCK-0134268	Email from Andrew Citro to (b)(3):6(f),(b)(4) (Nov. 4, 2014)
LIFELOCK-0134335	Email from Tim Oliver to (b)(3):6(f),(b)(4) (Sep. 26, 2014)
LIFELOCK-0134336	Email from (b)(3):6(f),(b)(4) to Tim Oliver (Oct. 3, 2014)
LIFELOCK-0134337-38	Email from Tim Oliver to (b)(3):6(f),(b)(4) (Jul. 16, 2014)
LIFELOCK-0134340	Email from (b)(3):6(f),(b)(4) (Oct. 16, 2014)
LIFELOCK-0134341	Email from Baneet Singh to (b)(3):6(f),(b)(4) (Oct. 15, 2014)
LIFELOCK-0134342	Email from (b)(3):6(f),(b)(4) to Tim Oliver (Oct. 17, 2014)
LIFELOCK-0134343-47	Email from (b)(3):6(f),(b)(4) to DL-Products & Technology Infrastructure, LifeLock (Oct. 2, 2014)
LIFELOCK-0134349	Email from (b)(3):6(f),(b)(4) to Tim Oliver (Sep. 26, 2014)
LIFELOCK-0134350	Email from (b)(3):6(f),(b)(4), Tim Oliver, Greg Beaubrun, Louis McNair, and (b)(3):6(f),(b)(4) (Oct. 6, 2014)
LIFELOCK-0134353	Email from (b)(3):6(f),(b)(4) (Oct. 6, 2014)
LIFELOCK-0134355	Email from (b)(3):6(f),(b)(4) to Tim Oliver (Oct. 31, 2014)
LIFELOCK-0134360-66	Email from (b)(3):6(f),(b)(4) Jul. 31, 2014)
LIFELOCK-0134369-370	Email from marketing@invincea.com to (b)(3):6(f),(b)(4) (Jul. 25, 2014)
LIFELOCK-0134371-77	Email from (b)(3):6(f),(b)(4) to (b)(3):6(f),(b)(4) (Aug. 1, 2014)
LIFELOCK-0134394	Email from to Slavko Jovanovic (Oct. 16, 2014)
LIFELOCK-0134395	Email from to Slavko Jovanovic (Oct. 16, 2014)
LIFELOCK-0134397	*UTS Pending/Open Requests*, generated by (b)(3):6(f),(b)(4) (Nov. 3, 2014)
LIFELOCK-0134402	Email from (b)(3):6(f),(b)(4) to Tim Oliver (Oct. 6, 2014)
LIFELOCK-0134403	Email from to Tim Oliver (Oct. 6, 2014)
LIFELOCK-0134404	Email from Tim Oliver to (b)(3):6(f),(b)(4) (Oct. 17, 2014)
LIFELOCK-0134407-08	Email from Tim Oliver to (Sep. 11, 2014)
LIFELOCK-0134409	Email from Tim Oliver to (b)(3):6(f),(b)(4) (Sep. 26, 2014)
LIFELOCK-0134435-441	*Open Vulnerability Remediation Requests – Windows*, generated by Austin Appel (Jul. 14, 2014)
LIFELOCK-0134484-85	Email from Matt Kennedy, (b)(3):6(f),(b)(4) (Jun. 17, 2014)
LIFELOCK-0134486-87	Email from Matt Kennedy, (b)(3):6(f),(b)(4) (Jun. 19, 2014)
LIFELOCK-0134488-	Email from Cyberheist News to (b)(3):6(f),(b)(4) (Oct. 28,

492	2014)
LIFELOCK-0134495	Email from (b)(3):6(f),(b)(4) to Rich Stebbins (Sep. 26, 2014)
LIFELOCK-0134496	Email from (b)(3):6(f),(b)(4) Resolution Manager, LifeLock to DL-Nicole Directs, LifeLock
LIFELOCK-0134534	*Untitled Document*
LIFELOCK-0134680-88	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Federal Trade Commission (Mar. 11, 2015)
LIFELOCK-0135517-588	*VRRs – Jun. 2012 to Sep. 2012 ARC Table with Notes. LifeLock*, generated by (b)(3):6(f),(b)(4) (May 5, 2015)
LIFELOCK-0135671-781	*VRRs – Apr. 2013 to Dec. 2014 ARC Table with Notes. LifeLock*, generated by (b)(3):6(f),(b)(4) (May 5, 2015)
LIFELOCK-0009498; 0034028-82; 0034099-101; 0034108; 0034122-24; 0034164-65; 0034252-53; 0034264-65	Documents Related to Risk Assessment Form 023
LIFELOCK-0075676; 0017100-02; 0020092-93; 0078701-02; 0078749; 0032489; 0100936; 0102384; 0096327; 0095646; 0032208; 0037396; 0025145; 0035976; 0010756; 0027040; 0026961; 0036021; 0037213	Documents Related to Risk Assessment Form 001
LIFELOCK-0053520-21; 00101589-590; 0101600-01; 0101831-32; 0079676-77; 0099922; 0102235-39; 0101667-69; 0101681-82; 0101998; 0101586-88; 0101835-38; 0102212-13; 0102240-42	Documents Related to Risk Assessment Form 002
LIFELOCK-0101829-30; 0100145-151; 0100216-221;	Documents Related to Risk Assessment Form 003

0081780-86; 0081764-771; 0034212-13; 0040892; 0105395-401; 0042286; 0107563-64; 0034214-15; 0032082-83; 0079722-730; 0078047-053; 0034185; 0034311-12; 0017268-273; 0040888; 0105377-384; 0034163; 0024049-054; 0033580-81; 0033894-99; 0042278; 0107546-51; 0052673-75; 0053834-38; 0102187-88; 0082277-78; 0078036-37; 0078449-450	
LIFELOCK-0009463-64; 0034070	Documents Related to Risk Assessment Form 007
LIFELOCK-0009465-66; 0082724	Documents Related to Risk Assessment Form 008
LIFELOCK-0009467-68; 0034133-34; --39814; 0103309; 0074962-64; 0075163-65	Documents Related to Risk Assessment Form 009
LIFELOCK-0034116-18; 0034362-63; 0034365-66; 0101829-30; 0100162-63; 0100145-151; 0100216-221; 0081780-86; 0081764-71; 0040892; 0105395-401; 0042286; 0107563-64; 0079722-730; 0096117; 0078047-53; 0101640-41; 0040888; 0105377-84; 0034399-401;	Documents Related to Risk Assessment Form 010

0042278; 0107546-51; 0053834-38; 0102187-88; 0082277-78; 0034373-75; 0078036-37; 0078449-50	
LIFELOCK-0009503-04; 0034212-13; 0040892; 0105395-401; 0042286; 0107563-64; 0034214-15; 0079722-730; 0101829-830; 0100162-63; 0100145-151; 0100216-221; 0081780-86; 0081764-771	Documents Related to Risk Assessment Form 011
LIFELOCK-0009500-01; 0034163; 0024049-054	Documents Related to Risk Assessment Form 012
LIFELOCK-0034203-05; 0034350-52; 0034167-69; 0033580-81; 0033894-99; 0042278; 0107546-551	Documents Related to Risk Assessment Form 013
LIFELOCK-0034187; 0034171; 0034316-20; 0034955-58; 0040983; 0105615-25; 0040979; 0105505-15; 0034384-89; 0034138-44; 0042983; 0108678-89; 0039805; 0105488-98; 0039788; 0103278-89; 0039783; 0103251-62; 0103233-44; 0034969-76; 0053834-38; 0034960-66; 0034196-202; 0034390-98	Documents Related to Risk Assessment Form 014
LIFELOCK-0009476-77; 0034176-77; 0034321-22	Documents Related to Risk Assessment Form 015
LIFELOCK-0009478-82; 0034094-95;	Documents Related to Risk Assessment Form 016

0034178-79; 0034323-24	
LIFELOCK-0009483-84; 0034180-81; 0034325-26	Documents Related to Risk Assessment Form 017
LIFELOCK-0009485-86; 0034190-91; 0034191; 0034327-28; 0078036-37	Documents Related to Risk Assessment Form 018
LIFELOCK-0034219-223; 0009487-88; 0013716-17; 0021090-91	Documents Related to Risk Assessment Form 019
LIFELOCK-0010010	VRR 81560
LIFELOCK-0030131-32	VRR 81561
LIFELOCK-0038581-82	VRR 81562
LIFELOCK-0038584-85	VRR 81563
LIFELOCK-0022582-83	VRR 81564
LIFELOCK-0010952-53	VRR 81565
LIFELOCK-0013015-16	VRR 81572
LIFELOCK-0013275-76	VRR 81573
LIFELOCK-0022612-13	VRR 81574
LIFELOCK-0024802-03	VRR 81575
LIFELOCK-0025121-22	VRR 81577
LIFELOCK-0030123-24	VRR 81578
LIFELOCK-0020432-33	VRR 81579
LIFELOCK-0026864-65	VRR 81580
LIFELOCK-0029168-69	VRR 81581

LIFELOCK-0023431-32	VRR 81582
LIFELOCK-0021107-08	VRR 81583
LIFELOCK-0020173-74	VRR 81584
LIFELOCK-0022182-83	VRR 81585
LIFELOCK-0030405-06	VRR 81586
LIFELOCK-0025947-48	VRR 81588
LIFELOCK-0026096-97	VRR 81589
LIFELOCK-0020012-13	VRR 84002
LIFELOCK-0010814-23	VRR 85243
LIFELOCK-0018181-82	VRR 87147
LIFELOCK-0015968-69	VRR 87343
N/A	Letter from Gregory Madden, Federal Trade Commission, to Andrew Berg, Counsel to LifeLock, Inc. (Dec. 12, 2014)
N/A	Letter from Andrew Berg, Counsel to LifeLock, Inc. to Gregory Madden, Federal Trade Commission (Dec. 24, 2014)
N/A	FTC REPORT V5 FINAL 20121116
N/A	Email from Sharon Schiavetti, Counsel to LifeLock, Inc., to Gregory Madden, Federal Trade Commission (Jun. 5, 2015)
LIFELOCK-0136811	*CR Tasks 05-13-15*, generated by (b)(3):6(f),(b)(4) (May 26, 2015)
LIFELOCK-0134689-759	Miscellaneous LifeLock Procedures Documents Produced to Federal Trade Commission

INDEX OF DOCUMENTS CITED
EXPERT REPORT OF DR. ERIC B. COLE

Attachment Number	Bates Number	Attachment Description
1	FTC-0002203-07	Curriculum Vitae of Dr. Eric Cole
2	FTC-0002009-29	Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants LifeLock and Davis (ECF No. 9, entered March 15, 2010)
3	FTC-0002208-28	Syllabus for *SEC401: Security Essentials*
4	FTC-0002229-40	Syllabus for *SEC501: Advanced Security Essentials – Enterprise Defender*
5	FTC-0002241-53	Syllabus for *SEC566: Implementing and Auditing the Critical Security Controls – In-Depth*
6	FTC-0002254-2342	*The Critical Security Controls for Effective Cyber Defense, Version 4.0*, Council on Cyber Security (2012)
7	FTC-0002094-2168	*Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, v. 2.0*, PCI Security Standards Council (Oct. 2010)
8	FTC-0002343-2741	*Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, National Institute of Standards and Technology (June 2010).
9	LIFELOCK 0053865-66	Email from (b)(3):6(f),(b)(4) *et al.* (Jul. 1, 2013)
10	LIFELOCK-0085248-50	Email from Gwen Ceylon to Tony Valentine (Jan. 17, 2013)
11	LIFELOCK-0038588-89	Email from Gwen Ceylon to Tony Valentine (Jan. 7, 2013)
12	LIFELOCK-0030131-32	Email from (b)(3):6(f),(b)(4) to Austin Appel (Jun. 6, 2013)
13	LIFELOCK-0135783-86, 0138077-78	LifeLock's VRR Logs (*322 Open Requests WO Tables with Notes*, generated by (b)(3):6(f),(b)(4) (May 27, 2015); *VRRs – June 2012 to September 2012 ARC Table with Notes*, generated by (b)(3):6(f),(b)(4) (May 29, 2015); *VRRs – October 2012 to March 2013 ARC Table with Notes*, generated by (b)(3):6(f),(b)(4) (May 29, 2015);

		VRRs – April 2013 to December 2014 ARC Table with Notes, generated by (b)(3):6(f),(b)(4) (May 29, 2015); *VRRs – April 2012 to May 2015 ARC Table with Notes*, generated by (b)(3):6(f),(b)(4) (May 29, 2015); *VRRs – April 2012 to May 2015 WO Table with Notes and Priority*, generated by (b)(3):6(f),(b)(4) (May 29, 2015)
14	LIFELOCK-0039701-07	LifeLock, Inc., PCI Audit Augmented Punch List (Jun. 11, 2013)
15	LIFELOCK-0053403-61	*LifeLock, Inc.: Information Assurance Services Enterprise Security Assessment,* Fishnet Security (Nov 13, 2012)
16	LIFELOCK-0025172-74	Email from (b)(3):6(f),(b)(4) *et al.* (Jul. 16, 2013)
17	LIFELOCK-97021-229	PCI Report on Compliance for LifeLock, Terra Verde Services (Jul. 2013)
18	LIFELOCK-00132479-516	LifeLock's Documentation of Penetration Test Vulnerability Remediation Submitted to (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) (submitted Jul. 2013)
19	LIFELOCK-0081949-56	Email from AnneMarie Olson to Michele Grant and (b)(3):6(f),(b)(4) (Oct. 11, 2013)
20	LIFELOCK-0032898-99	Email from Austin Appel to (b)(3):6(f),(b)(4) (Nov. 05, 2013)
21	LIFELOCK-0110772-81	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Attorney, Federal Trade Commission (Sept. 19, 2014)
22	LIFELOCK-2081-122	*LifeLock: Information Assurance Services Enterprise Security Assessment Report - Portal,* (b)(3):6(f),(b)(4) (Sept. 12, 2012)
23	LIFELOCK-0089119-120	Email from Jenner Holden to (b)(3):6(f),(b)(4) (Dec. 6, 2012)
24	LIFELOCK-0088573-74	Email from (b)(3):6(f),(b)(4) to Jenner Holden (Dec. 6, 2012)
25	LIFELOCK-0089186-87	Email from to Jenner Holden (Dec. 6, 2012)
26	LIFELOCK 0134378-85	Email from (b)(3):6(f),(b)(4) to (b)(3):6(f),(b)(4) (Aug. 1, 2014)
27	FTC-0002742-2851	Declaration of Elizabeth Anne Miles Pursuant to 28 U.S.C. § 1746
28	LIFELOCK-2123-81	*Final Report – LifeLock Security Review, Version 1.1,* (b)(3):6(f),(b)(4) (Sept. 21, 2012)
29	LIFELOCK-	LifeLock's Patching Logs

	0136812-13, 0138079-80	
30	FTC-0002874-2919	Declaration of Vinayak Balasubramanian Pursuant to 28 U.S.C. § 1746
31	FTC-0002169-2174	Letter from William C. MacLeod, Counsel to LifeLock, Inc., to Susan Pope, Federal Trade Commission (Jun. 12, 2015)
32	LIFELOCK-0138076	LifeLock's List of Decommissioned Servers (submitted on Jun. 12, 2015)
33	LIFELOCK-0019638-39	Email from (b)(3):6(f),(b)(4) to Rich Stebbins (Mar. 6, 2013)
34	LIFELOCK-0053824-25	Email from Austin Appel to David Bridgman and (b)(3):6(f),(b)(4) (Apr. 26, 2013)
35	LIFELOCK-0009259-61	LifeLock, Inc. PCI Audit Punch List (Apr. 19, 2013)
36	LIFELOCK-0134224-40	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Federal Trade Commission, (Jan. 2, 2015)
37	LIFELOCK-0088187-88	Email from Jenner Holden to Gwen Ceylon (Nov. 16, 2012)
38	LIFELOCK 77845	LifeLock PowerPoint Presentation, *Q2-Implement Monitoring Phase 1 Project (AP)* (2013)
39	LIFELOCK 33129-33133	Email from (b)(3):6(f),(b)(4) to Austin Appel (Apr. 03, 2013)
40	LIFELOCK 0034400-01	LifeLock, Security Exception Risk Assessment Form (Jun. 30, 2014)
41	LIFELOCK-0023835-36	Email from Loretta Stagnitto to Rich Stebbins *et al.* (May 13, 2013)
42	LIFELOCK 0077495-96	Email from Andy Doyle to Rich Stebbins (Sep. 30, 2013)
43	LIFELOCK 26183	Email from (b)(3):6(f),(b)(4) to Scott Watson *et al.* (Mar. 19, 2013)
44	LIFELOCK-0095891-959	*PCI DSS Gap Analysis Report*, (b)(3):6(f),(b)(4) (May 21, 2013)
45	LIFELOCK-0029627-28	Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Jul. 25, 2013)
46	LIFELOCK-0134215-16	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Federal Trade Commission (Dec. 9, 2014)
47	LIFELOCK-134056-65	Letter from Andrew Berg, Counsel to LifeLock, Inc., to Gregory Madden, Federal Trade Commission (Dec. 3, 2014)

48	LIFELOCK-3166-74	LifeLock Response to FTC 3/13/14 Information Request (Apr. 15, 2014)
49	FTC-0002852-60	C. Valladares, *PCI DSS Compliance: More Carrot and Less Stick?,* Tripwire.com (May 17, 2011)
50	FTC-0002861-69	E. Mills, *PCI compliance: What it is and why it matters (Q&A)*, CNET.com (Feb. 8, 2010)
51	LIFELOCK 24609-11	Email from Austin Appel to David Bridgman (Mar. 25, 2013)
52	LIFELOCK-0010367-74	Email from Tony Valentine to (b)(3):6(f),(b)(4) (Jul. 15, 2013)
53	LIFELOCK-0010416-18	LifeLock, Security Department Goals 2013 (Jan. 30, 2013)
54	LIFELOCK-0079743-44	LifeLock, 2014 Enterprise Risk Assessment Summary Report, by Anne Marie Olson (Mar. 12, 2014)
55	LIFELOCK-0135499-510	*DLA Piper, LLC - Digital Forensic Investigation Report,* (b)(3):6(f),(b)(4) (Nov. 26, 2014)
56	FTC-0002088-93	Adobe Systems, *Adobe Security Bulletin* (released on Apr. 28, 2014).
57	FTC-0002870-73	Symantec Corp., *Trojan.Cryptowall* (updated Mar. 3, 2015)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 1
TO EXPERT REPORT OF DR. ERIC B. COLE

Dr. Eric B. Cole
43605 Edison Club Ct
Ashburn, VA 20147
Tel: (703)-675-2055

Dr. Cole is an industry expert with breadth and depth experience across integrated cyber security. He focuses on creating, enhancing and growing technology based teams/organizations by bridging the gap between a business and technology mindset, with a focus on security and innovation.
Dr. Cole is an invited speaker, expert witness and member of many key organizations including member of the Commission on Cyber Security for the 44th President (25 industry experts), the Purdue University Executive Advisory Board and a senior fellow with SANS.

Summary of Professional Experience:

Secure Anchor Consulting Services: 2005-Present

Continuously execute on high-end consulting services to Fortune 500, Fortune 50, financial institutions, international organizations and the federal government. One of many assignments included a major system design and assessment for an international financial institution in Hong Kong. Continually stays abreast of cutting edge technology and technical components (network security, network architecture, and incident response, NOC/SOC design) to provide solutions that meet the business goals of an organization. Acts as an expert witness for several government and commercial companies in a variety of litigation (i.e. FTC vs. Microsoft and Nomadix vs. Second Rule). Frequently invited keynote speaker at a variety of conferences and security events around the world. Writes for a variety of publications and has authored several books.

McAfee: 2009-2010

SVP, CTO of the Americas

McAfee's visionary and evangelist responsible for strongly influencing the company's technical direction in alignment with our CEO, EVP, Product Operations and other key product executives and technologist across the world. Played an integral role in the company's strategic direction, development, and future growth as the global leader in digital security solutions. Key leader in the execution of technology strategy for technology platforms, partnerships, and external relationships. Worked closely with the CEO, EVP of Product Operations and other key stakeholders to establish a product vision and road map to achieve McAfee's goals and business strategies. Works closely with identifying and capturing intellectual property and driving new innovation across the company.

Lockheed Martin: 2005-2009

IS&GS Chief Scientist
LM Senior Fellow

The Sytex Group, Inc. (TSGI) was acquired by Lockheed Martin with a key component being the intellectual property created under the CTO leadership. Lockheed Martin selected Dr. Cole into its prestigious fellowship program, an award it makes to less than 1% of its 130,000 employees. Moreover, Dr. Cole was the first Fellow within Lockheed Martin's Information Technology Division. As a Lockheed Martin Senior Fellow, he is a frequently invited speaker at a variety of conferences and security events. As Lockheed Martin Chief Scientist, Dr. Cole's current role includes performing research and development to advance the state-of- the art in information

systems security. Dr. Cole specializes in: secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. Over his 5+ years at Lockheed Martin, he has played a lead technical advisory role in many high profile, security-focused projects for Federal clients to include civil, Intel and department of defense, including the FBI Sentinel, DHS Eagle, JPL, Hanford and FBI IATI programs. Dr. Cole brings Lockheed Martin clients the benefit of his wealth of information security knowledge, with demonstrated excellence spanning industry, academia, and government computing environments.

The Sytex Group, Inc. (TSGI): 2001-2005

Chief Technology Officer (CTO)

Positioned company to accomplish corporate growth and meeting financial targets by utilizing and enhancing technology. Work as an executive team to determine and implement technical direction and focus of company. Extensive experience with running projects including managing development efforts to exceed client requirements. Successfully created an intellectual property base (to include patents, journals, books and white papers) – this effort resulted in an overall increase in market value. The efforts of the research teams intellectual property increased advertising, market share and customer satisfaction through conferences, proposal and magazine articles. Maintained full accountability for revenue of $55million and indirectly involved in revenue of over $80 million. Provide continuous leadership to research team of over 20 people that creates intellectual property that competes and surpassed teams that were twenty times their size. Yearly patents were inline with the top 1000 producing patent companies in the United States. Develop and executed on creative techniques for influxing technology into non-technical business units to drive revenue and profit. Interfaces with government officials to include the pentagon, White House and Capital Hill and corporate executives to identify critical network security problems that need to be addressed and researched.

SANS Institute: 1999-Present

Dean of Faculty

Member of a 5 person team tasked with creating a degree granting institution and receiving certification from the state of Maryland. Currently offering two Master's degree program focused on technical people that need managerial skills and managers who need technical skills. Successfully passed first two phases of certification and should have official certification by the end of 2011. Designed and implemented curriculum and provide leadership to faculty to successful deliver the degrees.

SANS: 1999-Present

Director of Research-Computer Network Attack-Enterprise Security Architecture
Director of the Cyber Defense Initiative

Lead instructor and course developer for several security courses. One of the highest rated instructors and one of the few instructors that teaches a variety of courses. Executed and contributed to the development of several of the GIAC certifications including GIAC Certified Security Essentials (GSEC), GIAC Certified Advanced Incident Handling Analysts (GCIH) and GIAC Certified Firewall Analysts (GCFW). Responsible for staying up on technology and developing new course material that teaches students the state of the art in networking and security. Created and led several key efforts including the Levelone Notebook, top 10/20 vulnerability list and the Cyber defense initiative. Developed business plans for and created new technological initiatives. Constantly researched, tested and evaluated new security products and research efforts.

GraceIC: 2000-2001

Chief Security Officer (CSO)

Designed and executed in establishing GraceIC as a leader in the network security arena. Developed the product line and executed on the expertise to build the services. Provided management and gave direction to successfully delivery on technical skills of security employees. Provided leadership and implemented the proper internal security infrastructure within Grace such as secure email, proper protection of data and security policies. Presented at several national and international conferences and wrote several articles. Performed and documented research into the area of future applications and solutions to the network security problem that exists in the current market. Trained sales people, program managers and engineers on how to sell, manage and deliver security services. Maintained a pulse on technology in the market place to produce trending and markets plans.

American Institutes for Research: 1999-2000

Chief Information Officer (CIO)

Brought in to fix and revamp the entire IT infrastructure based on the organization having several security breaches, virus outbreaks and unreliable performance on the network. Within 3 months stabilized the entire IT infrastructure and within 9 months rebuilt the entire infrastructure. Network designed to achieve a balance between functionality and security while minimizing the monetary impact to the organization. After 1 year, there were no severe security breaches and all attempted breaches were contained prior to causing any significant monetary loss. Virus problems were contained and controlled and network uptime was 99.999%. Security and performance was greatly increased while overall IT costs were reduced by 15%. In addition, provided technical support for DARPA sponsored research projects.

Vista Information Technologies: 1998-1999

VP of Enterprise Security Services

Developed and executed the Enterprise Security Services Group and responsible for all internal and external security issues. Tracked and managed separate P&L (profit and loss) center for security. Grew the team from one person to over 12 people and executed on several million in annual revenue in less than a year. Setup the security and other monitoring services for the NOC/SOC. Created all of the security services offerings and generated all necessary marketing and sales material. Followed and assured compliance to business plan and financial tracking of security group. Performed security assessments and consult on all areas of security. Design, implement and monitor security solutions including firewall design, intrusion detection, vulnerability assessment and penetration testing. Performed evaluation and analysis of security tools and provided technical recommendations and product improvements for VC funded startups. Tracked on a large number of security and hacker tools. Key presenter at Cisco sponsored security seminars around the country and performed partnership activities with Fortune 500 organizations.

Teligent: 1996-1998

Director of Security

Created and in charge of IT Corporate Security Department. Central point of contact for all security concerns. Evaluate strategic plans and operational activities by performing risk assessment and determine how it might impact corporate security. Architected and designed security solutions to meet operational needs. Integrated security and help create NOC to provide for proper monitoring of network. Developed the company's security policy and all required security guidelines across the company. Setup an intrusion detection system for critical components of the network. Designed setup and maintained a perimeter network with PIX and Gauntlet firewalls. Setup security lab to properly test and enhance the security features of the network. Performed and executed on several computer investigations. Assisted and advised the legal department on researching laws, regulations, and policies relating to computer and

information security. Evaluated several secure email solutions and installed PGP Company wide. Established and setup web traffic monitoring and password tracking systems.

Central Intelligence Agency: 1991 - 1996

Received 6 Exceptional Performance Awards.

Program Manager / Technical Director for the Internet Program Team with Office of Technical Services

A Senior Officer of the agency that implemented the Internet Program Team that specializes in rapid development and in exploiting the latest Internet technologies that meet customer's requirements. The team designs, develops, tests, and deploys products in 3 to 6 month intervals. Designed and developed several secure communication systems. Responsible for providing technical direction, technical design, security assessment, and programming modules. Setup and maintained several servers (NT and Unix) and routers (Cisco 2500 and 3600 series). Secured internal servers, continually perform intrusion detection, and reviewed audit logs. Performed independent security reviews and penetration testing of (World Wide Web) servers for other offices. Identified several weaknesses and ways to fix those problems and secure the system. Currently, the team has had several successful deployments. Received letter of appreciation from the DCI (Director of Central Intelligence) and several Exceptional Performance Awards for this project.

Computer Engineer with Office of Security

Member of the information security assessment team. Evaluated and performed security assessment of network operating systems. Identified potential vulnerabilities and ways to secure the holes. Designed a large scale auditing system with automated review capability. Worked on several virus investigations.

Education:

Pace University - 2003

Doctorate degree in Network Security

M. S., New York Institute of Technology - 1993

Major: Computer Science
GPA: 4.0/4.0
Honors: Harry Schure Graduate Memorial Award (awarded to one graduating senior)

B.S., New York Institute of Technology - 1992

Major: Computer Science
Minor: Business
GPA: 3.7/4.0
Honors: Graduated Magna Cum Laude, Dorothy Schure Memorial Award, Jules Singer Award, Grace Hopper Award from Computer Associates, Presidential Academic Award (4.0 semesters), Presidential Service Award, Dean's List, Member of Who's Who Among Students in American Universities, and Member of Nu Ypsilon Tau Honor Society.

Certifications / Organizations

CISSP (Certified Information Systems Security Professional), MCSE (Microsoft Certified Systems Engineer), CCNA (Cisco Certified Network Associate) and ISS Internet Scanner and Real Secure Certification. Created several of the GIAC certification programs and exams.

Member of ACM, IEEE, International Who's Who in Information Technology, CSI Computer Security Institute), ISSA (Information Systems Security Association), and ICSA (International Computer Security Association). Member of the editorial board for CVE (Common vulnerability and exposures) and member of the HoneyNet project. Both are invitation only memberships. Author and speaker for SANS Institute

Publications

Network Security Bible, 2nd Edition

- **Paperback:** 936 pages
- **Publisher:** Wiley; 2 edition (September 8, 2009)
- **Language:** English
- **ISBN-10:** 0470502495
- **ISBN-13:** 978-0470502495
- **Product Dimensions:** 7.4 x 1.8 x 9.3 inches

Insider Threat

- **Paperback:** 350 pages
- **Publisher:** Syngress; 1 edition (March 1, 2006)
- **Language:** English
- **ISBN-10:** 1597490482
- **ISBN-13:** 978-1597490481
- **Product Dimensions:** 7 x 1.1 x 8.9 inches

Advanced Persistent Threat

- **Paperback:** 320 pages
- **Publisher:** Syngress; 1 edition (November 27, 2012)
- **Language:** English
- **ISBN-10:** 1597499498
- **ISBN-13:** 978-1597499491
- **Product Dimensions:** 7.5 x 0.6 x 9.2 inches

Monthly column on TechTarget - http://www.techtarget.com/contributor/Eric-Cole

Expert Witness Testimony at Trial or Deposition in Past 4 Years

National Union Fire Insurance Company of Pittsburgh, Pennsylvania v. Tyco Integrated Security, LLC et al., Case No. 13-080371-CIV-BLOOM/HUNT (S.D. Fla. filed Apr. 16, 2013)

Finjan, Inc. v. Blue Coat Systems, Inc., Case No. 13-cv-03999-BLF (N.D. Cal. filed Aug. 28, 2013)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 2
TO EXPERT REPORT OF DR. ERIC B. COLE

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Federal Trade Commission,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	
LifeLock, Inc.	)	
a corporation; Robert J. Maynard, Jr.,	)	**Civil No. CV10-530-PHX-NVW**
individually and as an officer of LifeLock,	)	
Inc.; and	)	**STIPULATED FINAL JUDGMENT AND**
Richard Todd Davis,	)	**ORDER FOR PERMANENT**
individually and as an officer of	)	**INJUNCTION AND OTHER**
LifeLock, Inc.,	)	**EQUITABLE RELIEF AS TO**
	)	**DEFENDANTS LIFELOCK AND DAVIS**
Defendants.	)	
	)	

STIPULATED FINAL JUDGMENT AND ORDER FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF AS TO DEFENDANTS LIFELOCK AND DAVIS

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), has concurrently filed its Complaint, which alleges that Defendants LifeLock, Inc. ("LifeLock"), Robert J. Maynard, Jr. ("Maynard"), and Richard Todd Davis ("Davis") have engaged in violations of Section 5 of the FTC Act, 15 U.S.C. § 45. The Commission and Defendants LifeLock and Davis ("Settling Defendants") have agreed to the entry of this Stipulated Final Judgment and Order for

Permanent Injunction and Other Equitable Relief ("Order") to resolve all matters in dispute in this action without trial or adjudication of any issue of law or fact herein and without Settling Defendants admitting the truth of, or liability for, any of the matters alleged in the Complaint. Settling Defendants have waived service of the Summons and Complaint.

THEREFORE, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter of this case and over Settling Defendants LifeLock and Davis.

2. Venue in this district is proper under 28 U.S.C. § 1391(b) and (c), and 15 U.S.C. § 53(b).

3. The acts and practices of Settling Defendants are in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

4. The Complaint states claims upon which relief may be granted against Settling Defendants under Sections 5 and 13(b) of the FTC Act, 15 U.S.C. §§ 45 and 53(b).

5. Settling Defendants make no admission to the allegations in the Complaint, other than the jurisdictional facts.

6. Settling Defendants waive: (a) all rights to seek appellate review or otherwise challenge or contest the validity of this Order; (b) any claim they may have against the Commission, its employees, representatives, or agents that relate to the matter stated herein; (c) all claims under the Equal Justice Act, 28 U.S.C. § 2412, as amended by Pub. L. 104-121, 110 Stat. 847, 863-64 (1996); and (d) any rights to attorneys' fees that may arise under said provision

of law.

7. Settling Defendants have entered into this Order freely and without coercion, and they acknowledge that they have read the provisions of this Order and are prepared to abide by them.

8. Entry of this Order is in the public interest.

9. LifeLock is concurrently agreeing to orders resolving related complaints brought by the Attorneys General of the States of Alaska, Arizona, California, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Missouri, Mississippi, Montana, Nebraska, Nevada, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, and West Virginia (the "Participating States"). These state orders will require LifeLock to pay $1 million to the Office of the Attorney General of Illinois for distribution among the Participating States.

DEFINITIONS

1. "Individual Defendant" shall mean Davis.

2. "Corporate Defendant" shall mean LifeLock, Inc. and its successors and assigns.

3. "Settling Defendants" shall mean Individual Defendant and Corporate Defendant, individually, collectively, or in any combination.

4. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen

name, that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and/or data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and/or check number; (h) a driver's license, military, or state identification number; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above.

5. "Subscribing Consumer" shall mean any person or entity that paid for Corporate Defendant's service at any time between April 1, 2005 and March 31, 2009.

ORDER

I. PROHIBITED BUSINESS ACTIVITIES

IT IS ORDERED that Settling Defendants and their officers, agents, servants, and employees and all persons in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or through any sole proprietorship, partnership, limited liability company, corporation, subsidiary, branch, division, or other entity, are hereby permanently restrained and enjoined from:

A. in connection with the advertising, distributing, promoting, offering for sale, or sale of any product, service, or program designed for the purpose of preventing, mitigating, or recovering from any form of identity theft as defined in 18 U.S.C. § 1028, misrepresenting in any manner, expressly or by implication:

1. that such product, service, or program provides complete protection against all forms of identity theft by making customers' personal

information useless to identity thieves;

2. that such product, service, or program prevents unauthorized changes to customers' address information;

3. that such product, service, or program constantly monitors activity on each of its customers' consumer reports;

4. that such product, service, or program ensures that a customer will always receive a phone call from a potential creditor before a new credit account is opened in the customer's name;

5. the means, methods, procedures, effects, effectiveness, coverage, or scope of such product, service, or program;

6. the risk of identity theft to consumers;

7. whether a particular consumer has become or is likely to become a victim of identity theft; and/or

8. the opinions, beliefs, findings, or experiences of an individual or group of consumers related in any way to any such product, service, or program.

Such products, services, or programs include, but are not limited to, the placement of fraud alerts on behalf of consumers, searching the internet for consumers' personal data, monitoring commercial transactions for consumers' personal data, identity theft protection for minors, and guarantees of any such products, services, or programs.

B. misrepresenting in any manner, expressly or by implication, the manner or extent to which they maintain and protect the privacy, confidentiality, or security of any personal information collected from or about consumers.

II. INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Corporate Defendant and any business entity that Individual Defendant controls, directly or indirectly, which collects, maintains, or stores personal information from or about consumers, shall, upon operation of this business, establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to the entity's size and complexity, the nature and scope of the entity's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;

C. the design and implementation of reasonable safeguards to control the risks

identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, system, and procedures;

D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information received from Settling Defendants and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of Settling Defendants' information security program in light of the results of the testing and monitoring required by Subsection C of this Section, any material changes to Settling Defendants' operations or business arrangements, or any other circumstances that Settling Defendants know or have reason to know may have a material impact on the effectiveness of their information security program.

III. BIENNIAL ASSESSMENT REQUIREMENTS

A. **IT IS FURTHER ORDERED** that Corporate Defendant and any business entity that Individual Defendant controls, directly or indirectly, which collects, maintains, or stores personal information from our about consumers, shall, in connection with their compliance with Section II of this Order, obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred eighty days after service of the Order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:

1. set forth the specific administrative, technical, and physical safeguards implemented and maintained during the reporting period;

2. explain how such safeguards are appropriate to Settling Defendants' size and complexity, the nature and scope of Settling Defendants' activities, and the sensitivity of the personal information collected from or about consumers;

3. explain how the safeguards that have been implemented meet or exceed the protections required by Section II of this Order; and

4. certify that Settling Defendants' security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

B. Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

C. Settling Defendants shall provide the initial Assessment within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Settling Defendants until the Order is terminated and provided to the Commission within ten (10) days of request.

IV. CONSUMER REDRESS

IT IS FURTHER ORDERED that:

A. Judgment in the amount of $35,000,000.00 is hereby entered jointly and severally against Settling Defendants. Full payment for the foregoing judgment is suspended, subject to the following conditions:

1. Corporate Defendant shall pay eleven million dollars ($11,000,000), which Corporate Defendant represents their undersigned counsel holds in escrow for no purpose other than payment to the Commission. Such payment shall be made within seven days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of the Commission.

2. Individual Defendant shall pay ten thousand dollars ($10,000), which Individual Defendant represents their undersigned counsel holds in escrow for no purpose other than payment to the Commission. Such payment shall be made within seven days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of the Commission.

B. In the event of any default in payment, which default continues for ten (10) days beyond the due date of payment, the entire unpaid amount, together with interest, as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall immediately become due and payable.

C. All funds paid to the FTC pursuant to the Order shall be deposited into an account administered by the Commission or its agent to be used for equitable relief which will include, but not be limited to, consumer redress, and any attendant expenses for the administration of

such equitable relief. Acceptance of redress from the FTC shall constitute an acknowledgment by the consumer that, to the extent that the consumer makes a subsequent claim, the defendant is entitled to deduct the amount of the redress received from the FTC from any other or additional redress ordered. Upon completion of consumer redress, Commission shall supply to Defendants the names of consumers that received redress and the amount received. In the event that funds remain after redress is attempted, the Commission may apply any remaining funds for such other equitable relief (including consumer information remedies) as it determines to be reasonably related to Settling Defendants' practices alleged in the Complaint. Any funds not used for such equitable relief shall be deposited to the United States Treasury as disgorgement. Settling Defendants shall have no right to challenge the Commission's choice of remedies under this Section. Settling Defendants shall have no right to contest the manner of distribution chosen by the Commission.

D. Settling Defendants relinquish all dominion, control, and title to the funds paid to the fullest extent permitted by law. Settling Defendants shall make no claim to or demand return of the funds, directly or indirectly, through counsel or otherwise.

E. Settling Defendants agree that the facts as alleged in the Complaint filed in this action shall be taken as true without further proof in any bankruptcy case or subsequent civil litigation pursued by the Commission to enforce its rights to any payment or money judgment pursuant to this Order, including but not limited to a nondischargeability complaint in any bankruptcy case. Settling Defendants further stipulate and agree that the facts alleged in the Complaint establish all elements necessary to sustain an action pursuant to, and that this Order shall have collateral estoppel effect for purposes of, Section 523(a)(2)(A) of the Bankruptcy

Code, 11 U.S.C. § 523(a)(2)(A).

F. Settling Defendants shall, within ten (10) days of the date of entry of this Order, provide to the Commission, an encrypted file containing, in Access database format, for each Subscribing Consumer: (1) the consumer's name; (2) most recent known mailing address, e-mail address, and telephone number; (3) the beginning and end date for the consumer's subscription to the service; and (4) the monthly rate paid by the consumer. The database shall be formatted with a separate field for each piece of information requested, and, for the mailing address, separate fields for street number, building/apartment number, city, state, and zip code. Settling Defendants shall cooperate in good faith with the Commission or its representative to obtain and provide any additional information required to administer consumer redress and take all reasonable steps to ensure that all data provided is accurate, up-to-date, and in a secure and useable format. In the event the Defendants fail to provide data that is accurate, up-to-date, and in a secure and useable format, the Commission may apply any remaining funds for such other equitable relief (including consumer information remedies) as it determines to be reasonably related to Settling Defendants' practices alleged in the Complaint. Any funds not used for such equitable relief shall be deposited to the United States Treasury as disgorgement.

V. RIGHT TO REOPEN AS TO MONETARY JUDGMENT

IT IS FURTHER ORDERED that the Commission's agreement to this Order is expressly premised upon the truthfulness, accuracy and completeness of Settling Defendants' sworn financial statements and supporting documents submitted to the Commission, which include material information upon which the Commission relied in negotiating and agreeing to this Order. If, upon motion by the Commission, this Court finds that any Settling Defendant has

failed to disclose any material asset, or materially misstated the value of any asset in the financial statements and information submitted to the Commission, or has made any other material misstatement or omission in the financial statements and related documents described above, then this Order shall be reopened and suspension of the judgment against that particular Settling Defendant shall be lifted for the purpose of requiring payment in the full amount of the judgment ($35,000,000). Provided, however, that in all other respects this Order shall remain in full force and effect, unless otherwise ordered by the Court.

VI. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of (i) monitoring and investigating compliance with any provision of this Order, and (ii) investigating the accuracy of any Settling Defendant's financial statements upon which the Commission's agreement to this Order is expressly premised:

A. Within ten (10) days of receipt of written notice from a representative of the Commission, Settling Defendants each shall submit additional written reports, which are true and accurate and sworn to under penalty of perjury; produce documents for inspection and copying; appear for deposition; and provide entry during normal business hours to any business location in each Settling Defendant's possession or direct or indirect control to inspect the business operation;

B. In addition, the Commission is authorized to use all other lawful means, including but not limited to:

1. obtaining discovery from any person, without further leave of court, using the procedures prescribed by Fed. R. Civ. P. 30, 31, 33, 34, 36, 45 and 69;

2. posing as consumers and suppliers to Settling Defendants, their employees, or any other entity managed or controlled in whole or in part by any Settling Defendant, without the necessity of identification of prior notice; and

C. Settling Defendants each shall permit representatives of the Commission to interview any employer, consultant, independent contractor, representative, agent, or employee who has agreed to such an interview, relating in any way to any conduct subject to this Order. The person interviewed may have counsel present.

Provided however, that nothing in this Order shall limit the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. § § 49, 57b-1, to obtain any documentary material, tangible things, testimony, or information relevant to unfair or deceptive acts or practices in or affecting commerce (within the meaning of 15 U.S.C. § 45(a)(1)).

VII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that, in order that compliance with the provisions of this Order may be monitored:

A. For a period of five (5) years from the date of entry of this Order for Corporate Defendant and a period of three (3) years from the date of entry of this Order for Individual Defendant,

1. Individual Defendant shall notify the Commission of the following:

a. Any changes in Individual Defendant's residence, mailing addresses, and telephone numbers, within ten (10) days of the date of the change;

b. Any changes in Individual Defendant's employment status (including self-employment), and any change in Individual Defendant's ownership in any business entity, within ten (10) days of the date of such change. Such notice shall include the name and address of each business that Individual Defendant is affiliated with, employed by, creates or forms, or performs services for; a detailed description of the nature of the business; and a detailed description of Individual Defendant's duties and responsibilities in connection with the business or employment; and

c. Any changes in Individual Defendant's name or use of any aliases or fictitious names.

2. Settling Defendants shall notify the Commission of any changes in structure of Corporate Defendant or any business entity that any Defendant directly or indirectly controls, or has ownership interest in, that may affect compliance obligations under this Order, including but not limited to: incorporation or other organization; a dissolution, assignment, sale, merger, or other action; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; or a change in the business name or address, at least thirty (30) days prior to such change, *provided* that, with respect to any proposed change in the business entity which a Defendant learns less than thirty (30) days prior to the date such action is to take place, such Defendant shall notify the Commission as soon as practicable after obtaining such knowledge.

B. One hundred eighty (180) days after the date of entry of this Order and annually

thereafter for a period of five (5) years for Corporate Defendant and three (3) years for Individual Defendant, Settling Defendants each shall provide a written report to the FTC, which is true and accurate and sworn to under penalty of perjury, setting forth in detail the manner and form in which they have complied and are complying with this Order. This report shall include, but not be limited to:

1. For Individual Defendant:

   a. Individual Defendant's then-current residence address, mailing address, and telephone numbers;

   b. Individual Defendant's then-current employment status (including self-employment), including the name, addresses, and telephone numbers of each business that Individual Defendant is affiliated with, employed by, or performs services for; a detailed description of the nature of the business; and a detailed description of Individual Defendant's duties and responsibilities in connection with the business or employment; and

   c. Any other changes required to be reported under Subsection A of this Section.

2. For all Settling Defendants:

   a. A copy of each acknowledgment of receipt of this Order, obtained pursuant to the Section titled "Distribution of Order;"

   b. Any other changes required to be reported under Subsection A of this Section.

C. Each Defendant shall notify the Commission of the filing of a bankruptcy petition by such Defendant within fifteen (15) days of filing.

D. For the purposes of this Order, Settling Defendants shall, unless otherwise directed by the Commission's authorized representatives, send by overnight courier all reports and notifications required by this Order to the Commission, to the following address:

Associate Director for Enforcement
Federal Trade Commission
600 Pennsylvania Avenue, N.W., Room NJ-2122
Washington, D.C. 20580
RE: FTC v. LifeLock, Inc.

Provided that, in lieu of overnight courier, Settling Defendants may send such reports or notifications by first-class mail, but only if Settling Defendants contemporaneously send an electronic version of such report or notification to the Commission at: DEBrief@ftc.gov.

E. For purposes of the compliance reporting and monitoring required by this Order, the Commission is authorized to communicate directly with each Defendant.

VIII. RECORD KEEPING PROVISIONS

IT IS FURTHER ORDERED that Settling Defendants and their agents, employees, officers, corporations, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, in connection with, are hereby restrained and enjoined from failing to create and retain the following records for the following periods:

A. For a period of eight (8) years from the date of entry of this Order for Corporate Defendant and six (6) years from the date of entry of this Order for Individual Defendant, the following records in connection with the sale or provision of products or services related to

identity theft:

1. Accounting records that reflect the cost of goods or services sold, revenues generated, and the disbursement of such revenues;
2. Personnel records accurately reflecting: the name, address, and telephone number of each person employed in any capacity by such business, including as an independent contractor; that person's job title or position; the date upon which the person commenced work; and the date and reason for the person's termination, if applicable;
3. Customer files containing the names, addresses, phone numbers, dollar amounts paid, quantity of items or services purchased, and description of items or services purchased, to the extent such information is obtained in the ordinary course of business;
4. Complaints and refund requests (whether received directly, indirectly, or through any third party) and any responses to those complaints or requests;
5. Copies of all sales scripts, training materials, advertisements, or other marketing materials;
6. Any documents, whether prepared by or on behalf of Settling Defendants, that contradict, qualify, or call into question Settling Defendants' compliance with Sections I, II, and III of this Order; and
7. All records and documents necessary to demonstrate full compliance with each provision of this Order, including but not limited to, copies of

acknowledgments of receipt of this Order required by the Sections titled "Distribution of Order" and "Acknowledgment of Receipt of Order" and all reports submitted to the FTC pursuant to the Section titled "Compliance Reporting;"

B. For a period of three (3) years after the date of preparation of each Assessment required under the Section titled "Biennial Assessment Requirements": All materials relied upon to prepare the Assessment, whether prepared by or on behalf of any Settling Defendant, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Settling Defendants' compliance with the Section titled "Biennial Assessment Requirements."

IX. DISTRIBUTION OF ORDER

IT IS FURTHER ORDERED that for a period of five (5) years from the date of entry of this Order for Corporate Defendant and three (3) years from the date of entry of this Order for Individual Defendant, Settling Defendants shall deliver copies of the Order as directed below:

A. Corporate Defendant: Corporate Defendant must deliver a copy of this Order to (1) all of its principals, officers, directors, and managers; (2) all of its employees, agents, and representatives who engage in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting." For current personnel, delivery shall be within five (5) days of service of this Order upon such Defendant. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting," delivery shall

be at least ten (10) days prior to the change in structure.

B. Individual Defendant as Control Person: For any business that Individual Defendant controls, directly or indirectly, or in which Individual Defendant has a majority ownership interest, Individual Defendant must deliver a copy of this Order to (1) all principals, officers, directors, and managers of that business; (2) all employees, agents, and representatives of that business who engage in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting." For current personnel, delivery shall be within five (5) days of service of this Order upon such Defendant. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled "Compliance Reporting," delivery shall be at least ten (10) days prior to the change in structure.

C. Individual Defendant as employee or non-control person: For any business where Individual Defendant is not a controlling person of a business but otherwise engages in conduct related to the subject matter of this Order, such Individual Defendant must deliver a copy of this Order to all principals and managers of such business before engaging in such conduct.

D. Settling Defendants must secure a signed and dated statement acknowledging receipt of the Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this Section.

X. ACKNOWLEDGMENT OF RECEIPT OF THIS ORDER

IT IS FURTHER ORDERED that each Defendant, within five (5) business days of receipt of this Order as entered by the Court, must submit to the Commission a truthful sworn

statement acknowledging receipt of this Order.

XI. COOPERATION WITH COMMISSION COUNSEL

IT IS FURTHER ORDERED that the Settling Defendants shall, in connection with this action or any subsequent investigation related to or associated with the transaction or the occurrences that are the subject of the Complaint, cooperate in good faith with the Commission and appear at such places and times as the Commission shall reasonably request, after written notice, for interviews, conferences, pretrial discovery, review of documents, and for such other matters as may be reasonably requested by the Commission. If requested in writing by the Commission, the Settling Defendants shall appear or cause their officers, employees, representatives or agents to appear, and provide truthful testimony in any trial, deposition, or other proceeding related to or associated with the transactions or the occurrences that are the subject of the Complaint, without the service of a subpoena.

XII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

XIII. COSTS AND ATTORNEYS' FEES

IT IS FURTHER ORDERED that each party shall bear its own costs and attorneys' fees incurred in connection with this action.

XIV. NOTICE OF ENTRY OF ORDER

IT IS FURTHER ORDERED that entry in the docket of this Order by the Clerk of Court shall constitute notice to Settling Defendants of the terms and conditions of this Order, and that Settling Defendants waive all rights to contest in any future proceeding whether Settling Defendants were properly served with this Order.

The parties hereby stipulate to the entry of the foregoing Order, which shall constitute a final Order in this action.

IT IS SO ORDERED:

DATED this 15th day of March, 2010.

Neil V. Wake
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 3
TO EXPERT REPORT OF DR. ERIC B. COLE

Trust the CLOUD for sensitive info? Take Survey & Enter to Win $400 Amazon Card

SEC401: Security Essentials Bootcamp Style

Contents | Additional Info

Delivery Methods:
Live | Online

GSEC Certification
Affiliate Pricing
46 CPEs
Laptop Required

Masters Program

Very well rounded. Great that he(the instructor)was able to bring real world examples to class. Made the class flow smoothly.
Robin Mahon, Kapstone Paper

SEC401 provides an excellent overview of security fundamentals delivered by experienced industry professionals.
Jathan Watso, Department of Finance

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is SEC401: Security Essentials Bootcamp Style the right course for you?

STOP and ask yourself the following questions:

1. Do you fully understand why some organizations get compromised and others do not?
2. If there were compromised systems on your network, are you confident that you would be able to find them?
3. Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
4. Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, SEC401 course will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

More

Assessment Available

FTC-0002208

Test your security knowledge with our free SANS Security Essentials Assessment Test.

[redacted]

Notice: This course prepares you for the GSEC certification that meets the requirement of the DoD 8570 IAT Level 2.

Course Content Overlap Notice: Please note that some course material for SEC401 and MGT512 may overlap. We recommend SEC401 for those interested in a more technical course of study, and MGT512 for those primarily interested in a leadership-oriented but less technical learning experience.

Course Syllabus

Collapse All

Course Contents

SEC401.1: Networking Concepts

Overview

A key way that attackers gain access to a company's resources is through a network connected to the Internet. A company wants to try to prevent as many attacks as possible, but in cases where it cannot prevent an attack, it must detect it in a timely manner. Therefore, an understanding of how networks and the related protocols like TCP/IP work is critical to being able to analyze network traffic and determine what is hostile. It is just as important to know how to protect against these attacks using devices such as routers and firewalls. These essentials, and more, will be covered during this course day in order to provide a firm foundation for the consecutive days of training.

CPE/CMU Credits: 8

Topics

Setting Up a Lab with Virtual Machines

- Use
- Implementation
- Security

Network Fundamentals

- Network types (LANs, WANs)
- Network topologies
- LAN protocols
- WAN protocols
- Network devices

IP Concepts

- Packets and addresses
- IP service ports
- IP protocols
- TCP
- UDP
- ICMP
- DNS

IP Behavior

- TCP dump

FTC-0002209

- Recognizing and understanding
- UDP
- ICMP
- UDP behavior

Virtual Machines

- Use
- Implementation
- Security

SEC401.2: Defense In-Depth

Overview

To secure an enterprise network, you must have an understanding of the general principles of network security. In this course, you will learn about six key areas of network security. The day starts with information assurance foundations. Students look at both current and historical computer security threats, and how they have impacted confidentiality, integrity, and availability. The first half of the day also covers creating sound security policies and password management, including tools for password strength on both Unix and Windows platforms. The second half of the day is spent on understanding the information warfare threat and the six steps of incident handling. The day draws to a close by looking at attack strategies and how the offense operates.

CPE/CMU Credits: 8

Topics

Information Assurance Foundations

- Defense in-depth
- Confidentiality, integrity, and availability
- Risk model
- Authentication vs. authorization
- Vulnerabilities
- Defense in-depth

Computer Security Policies

- Elements when well written
- How policies serve as insurance
- Roles and responsibilities

Contingency and Continuity Planning

- Business continuity planning (BCP)
- Disaster recovery planning (DRP)
- Business impact analysis

Access Control

- Data classification
- Authentication, authorization, accountability (AAA)
- MAC and DAC

Password Management

- Password cracking for Windows and Unix
- Alternate forms of authentication (tokens, biometrics)
- Single sign-on and RADIUS

Incident Response (IR)

- Preparation, identification, and containment

- Eradication, recovery, and lessons learned
- Investigation techniques and computer crime
- Legal issues associated with IR

Offensive and Defensive Information Warfare (IW)

- Types of IW
- APT
- Asymmetric warfare
- Offensive goals

Attack Strategies and Methods

- How the adversary breaks into systems
- Mitnick attack
- Attack methods

SEC401.3: Internet Security Technologies

Overview

Military agencies, banks, and retailers offering electronic commerce programs, as well as dozens of other types of organizations, are striving to understand the threats they are facing and what they can do to address those threats. On day 3, you will be provided with a roadmap to help you understand the paths available to organizations that are considering deploying or planning to deploy various security devices and tools such as intrusion detection systems and firewalls. When it comes to securing your enterprise, there is no single technology that is going to solve all your security issues. However, by implementing an in-depth defense strategy that includes multiple risk-reducing measures, you can go a long way toward securing your enterprise.

CPE/CMU Credits: 8

Topics

Vulnerability Scanning and Remediation

- Approaches and methods of remediation
- Building a network visibility map
- Host identification
- Port scanning
- Vulnerability scanning
- Penetration testing

Web Security

- Web communication
- Web security protocols
- Active content
- Cracking web applications
- Web application defenses

Firewalls and Perimeters

- Types of firewalls
- Pros and cons of firewalls
- Firewall placement
- Packet filtering, stateful, and proxies

Honeypots

- Forensics
- Honeypots
- Honeynets
- Honey tokens

FTC-0002211

Host-based Protection

- Intrusion detection
- Intrusion prevention
- Tripwire
- Pros and cons

Network-based Intrusion Detection and Prevention

- Pros and cons
- Deployment strategies
- Snort
- Development and advances

SEC401.4: Secure Communications

Overview

There is no silver bullet when it comes to security. However, there is one technology that would help solve a lot of security issues, though few companies deploy it correctly. This technology is cryptography. Concealing the meaning of a message can prevent unauthorized parties from reading sensitive information. Day **4** looks at various aspects of encryption and how it can be used to secure a company's assets. A related area called steganography, or information hiding, is also covered. The day finishes by looking at using the Critical Security Controls for metrics based dashboards and performing risk assessment across an organization.

CPE/CMU Credits: 8

Topics

Cryptography

- Need for cryptography
- Types of encryption
- Symmetric
- Asymmetric
- Hash
- Ciphers
- Digital substitution
- Algorithms
- Real-world cryptosystems
- Crypto attacks
- VPNs
- Types of remote access
- PKI
- Digital certificates
- Key escrow

Steganography

- Types
- Applications
- Detection

Critical Security Controls

- Overview of the controls
- Implementing the controls
- Auditing the Controls
- Specific controls and metrics

Risk Assessment and Auditing

FTC-0002212

Risk assessment methodology
- Risk approaches
- Calculating risk
- SLE
- ALE

SEC401.5: Windows Security

Overview

Windows is the most widely-used and hacked operating system on the planet. At the same time, the complexities of Active Directory, PKI, BitLocker, AppLocker, and User Account Control represent both challenges and opportunities. This section will help you quickly master the world of Windows security while showing you the tools that can simplify and automate your work. You will complete the day with a solid grounding in Windows security, by looking at automation, auditing and forensics.

CPE/CMU Credits: 8

Topics

Security Infrastructure

- Windows family of operating systems
- Workgroups and local accounts
- What is Active Directory?
- Domain users and groups
- Kerberos, NTLMv2, smart cards
- Forests and trusts
- What is group policy?

Service Packs, Patches, and Backups

- Service packs
- E-mail security bulletins
- Patch installation
- Automatic updates
- Windows server update services
- Windows backup
- System restore
- Device driver rollback

Permissions and User Rights

- NTFS permissions
- File and print sharing service
- Shared folders
- BitLocker drive encryption

Security Policies and Templates

- Group policy objects
- Password policy
- Lockout policy
- Anonymous access
- Software restriction policies

Securing Network Services

- Firewalls and packet filtering
- IPSec and VPNs
- Wireless networking
- Security configuration wizard
- Remote desktop protocol (RDP)

Auditing and Automation

- Microsoft baseline security analyzer
- SECEDIT.EXE
- Windows event logs
- NTFS and registry auditing
- IIS logging
- Creating system baselines
- Scripting tools
- Scheduling jobs

SEC401.6: Unix/Linux Security

Overview

While organizations do not have as many Unix/Linux systems, those that they do have are often some of the most critical systems that need to be protected. Day 6 provides step-by-step guidance to improve the security of any Linux system. The course combines practical "how to" instructions with background information for Linux beginners, as well as security advice and best practices for administrators of all levels of expertise.

CPE/CMU Credits: 6

Topics

Linux Landscape

- Different variants of and uses for Linux
- Ways processes are started
- Network interface information
- Process information
- Directory hierarchy
- Partitions and OS installation

Permissions and User Accounts

- Setting permissions
- SUID and SGID
- Controlling access
- Root vs. user accounts
- Setting password controls
- Pluggable authentication module (PAM)

Linux OS Security

- Dangerous services
- Helpful services
- Running and stopping programs
- Configuration changes and restarting services
- File system permissions, ownership, and systems
- Mounting drives

Maintenance, Monitoring, and Auditing Linux

- Common causes of compromise
- Patching
- Backing up data
- Syslog
- Analyzing log files
- Other logging

FTC-0002214

Linux Security Tools

- File integrity verifications
- Chkrootkit
- CIS hardening guides
- Bastille linux
- Sniffers
- Snort

Additional Information

Testimonial

To give you an idea of the effectiveness of the course, here is what a few former students have said about it:

"SEC401 provides an excellent overview of security fundamentals delivered by experienced industry professionals." - *Jathan Watso, Department of Finance*

"Excellent material for security professionals wanting a deeper level of knowledge on how to implement security policies, procedures, and defensive mechanisms in an org." - *Brandon Smit, Dynetics*

"SEC401 took what I thought I knew and truly explained everything to me. Now, I also UNDERSTAND the security essentials fundamentals and how/why we apply them. Loved the training, cannot wait to come back for more." - *Nicholas Blanton, ManTech International*

Laptop Required

Security 401: Security Essentials Bootcamp Style consists of course instructions and hands-on sessions. To reinforce the skills covered in class and gain experience with the tools needed to implement effective security, there are hands-on labs every day. These lab sessions are designed to enable students to use the knowledge gained throughout the course in an instructor-led environment. Students will have the opportunity to install, configure, and utilize the tools and techniques that they have learned.

Students will require a system running Windows 8.x and Kali Linux with the following requirements:

- Administrator access to the operating system and all security software installed. Changes need to be made to personal firewalls and other host-based software in order for the labs to work.
- Anti-virus software will need to be disabled in order to install some of the tools.
- A DVD player is required to install the tools that will be provided in class.

Students are required to bring their own laptops that are properly configured. There is not enough time in class to help you install your laptop, so please note that your laptop must be properly installed and configured before you come to class. Students are also required to test their systems prior to coming to class. Do not bring a regular production laptop to this class! When installing software, there is always a chance of breaking something else on the system. Students should assume that all data could be lost.

Students must bring a laptop with Windows 8.x installed. The recommended configuration is Windows 8 as the host operating system running Kali Linux as a virtual machine with VMWare Player. Students can use a Mac or Linux system with a different virtual machine product running both Windows and Kali Linux on virtual machines, but the specific details for setting it up are left to the student.

Students MUST also download/install VMWare Player and Kali Linux prior to coming to class.

The following is a step by step guide for configuring your system on a Windows platform: SEC401 Installation Guide.

In summary, before you arrive for the course you should:

- Confirm that Windows 8.x is installed and working
- Download and install VMWare Player
- Install Kali Linux
- Confirm that you can start up Kali Linux and run a program.

NOTE: All of the screen shots that show installation and running of the tools are in Window 8. The labs are written for Windows 8; however all of the tools will run in windows 7 and the screen shots for running the tools are the same. The only difference is since there is no start menu in Windows 8 the method for accessing a DVD and initially running a program are different. If you know how to open a DVD and run a program in Windows 7, you will be able to use Windows 7 for the labs.

By properly preparing, you will have a knowledge-rich and enjoyable lab experience.

If you have any questions, feel free to contact us.

Sincerely,

Dr. Eric Cole

Track Lead/Course Author

E-mail: eric@sans.org

If you have additional questions about the laptop specifications, please contact laptop_prep@sans.org.

Who Should Attend

Anyone who works in security, is interested in security, or has to understand security should take this course, including:

- Security professionals who want to fill the gaps in their understanding of technical information security
- Managers who want to understand information security beyond simple terminology and concepts
- Operations personnel who do not have security as their primary job function but need an understanding of security to be effective
- IT engineers and supervisors who need to know how to build a defensible network against attacks
- Administrators responsible for building and maintaining systems that are being targeted by attackers
- Forensic analysts, penetration testers, and auditors who need a solid foundation of security principles so they can be as effective as possible at their jobs
- Anyone new to information security with some background in information systems and networking.

Prerequisites

SEC401 Security Essentials Bootcamp Style covers all of the core areas of security and assumes a basic understanding of technology, networks, and security. For those who are brand new to the field with no background knowledge, SEC301: Intro to Information Security would be the recommended starting point. While SEC301 is not a prerequisite, it will provide the introductory knowledge that will help maximize the experience with SEC401.

Other Courses People Have Taken

Other Courses People Have Taken

For those who are more advanced, SEC501: Enterprise Defender might be the more appropriate course to take.

What You Will Receive

In this course you will receive the following materials:

- Course books with labs
- Glossary and acronym list
- DVD
- TCP/IP reference guide

You Will Be Able To

- Apply what you learned directly to your job when you go back to work
- Design and build a network architecture using VLANs, NAC, and 802.1x based on advanced persistent threat indicators of compromise
- Run Windows command line tools to analyze the system looking for high-risk items
- Run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools
- Install VMWare and create virtual machines to create a virtual lab to test and evaluate tools/security of systems
- Create an effective policy that can be enforced within an organization and design a checklist to validate security and create metrics to tie into training and awareness
- Identify visible weaknesses of a system using various tools and, once vulnerabilities are discovered, cover ways to configure the system to be more secure
- Build a network visibility map that can be used for hardening of a network - validating the attack surface and covering ways to reduce that surface by hardening and patching
- Sniff open protocols like telnet and ftp and determine the content, passwords, and vulnerabilities using WireShark.

Hands-on Training

SEC401 is an interactive hands-on training course. The following are some of the lab activities that students will carry out:

- Setup of virtual lab environment
- Windows/Linux tutorial
- TCP dump analysis
- WireShark decoding of VoIP traffic
- Password cracking
- Host-based discovery with Dumpsec
- Hashing to preserve digital evidence
- Analyzing networks with hping and nmap
- Event correlation with Splunk
- Use of steganography tools
- Securing a Windows system with MBSA and SCA

Author Statement

"One of the things I love to hear from students after teaching Security 401 is 'I have worked in security for many years and after taking this course I realized how much I did not know.' With the latest version of Security Essentials and the Bootcamp, we have really captured the critical aspects of security and enhanced those topics with examples to drive home the key points. After you have attended Security 401, I am confident you will walk away with solutions to problems you have had for a while, plus solutions to problems you did not even know you had."

- Eric Cole

Additional Resources

View Dr. Cole's security videos

Learn even more about computer and information security in the SANS Reading Room, where more than 1,600 White Papers authored by industry professionals are available for free. The papers cover such topics as:

- Network fundamentals
- Core security design principles for networks
- Protocol behavior
- Analysis and decoding of packets
- Information assurance foundations
- Computer security policies
- Contingency and continuity planning
- Password management and access control
- Incident handling
- Offensive and defensive information warfare
- Host-based intrusion detection and prevention
- Network-based intrusion detection and prevention
- Offensive methods of attack
- Firewalls and perimeters
- Risk assessment and auditing
- Cryptography

- Steganography
- Wireless security
- Operations security
- Windows security
- Unix/Linux security

Take your learning beyond the classroom. Explore our site network for additional resources related to this course's subject matter.

Cyber Defense

**CPE/CMU credits not offered for the SelfStudy delivery method*

Online options available. Train from any location. OnDemand vLive

61 Training Results

All | Training Events | Community SANS | Mentor | Virtual | Online

Type	Topic	Course / Location / Instructor	Date	Register
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS London in the Summer 2015 London, United Kingdom Stephen Sims	Jul 13, 2015 - Jul 18, 2015	WAITLIST Waiting List
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS San Jose 2015 San Jose, CA Bryan Simon	Jul 20, 2015 - Jul 25, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Minneapolis 2015 Minneapolis, MN Russell Eubanks	Jul 20, 2015 - Jul 25, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Boston 2015 Boston, MA	Aug 3, 2015 - Aug 8, 2015	Register Now

FTC-0002219

		Ted Demopoulos		
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS San Antonio 2015 San Antonio, TX Keith Palmgren	Aug 17, 2015 - Aug 22, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Virginia Beach 2015 Virginia Beach, VA Dr. Eric Cole	Aug 24, 2015 - Sep 4, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Chicago 2015 Chicago, IL Paul A. Henry	Aug 30, 2015 - Sep 4, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Milan 2015 Milan, Italy Bryan Simon	Sep 7, 2015 - Sep 12, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Crystal City 2015 Crystal City, VA Tim Garcia	Sep 8, 2015 - Sep 13, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Network Security 2015 Las Vegas, NV Dr. Eric Cole	Sep 12, 2015 - Sep 21, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Baltimore 2015 Baltimore, MD Paul A. Henry	Sep 21, 2015 - Sep 26, 2015	Register Now
		SEC401: Security Essentials Bootcamp Style		

FTC-0002220

Training Event	Essentials	SANS Seattle 2015 Seattle, WA Bryce Galbraith	Oct 5, 2015 - Oct 10, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SOS: SANS October Singapore 2015 Singapore, Singapore Mark Hofman	Oct 12, 2015 - Oct 24, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Tysons Corner 2015 Tysons Corner, VA Bryan Simon	Oct 12, 2015 - Oct 17, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Gulf Region 2015 Dubai, United Arab Emirates Jonathan Ham	Oct 17, 2015 - Oct 29, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Cyber Defense San Diego 2015 San Diego, CA Dr. Eric Cole	Oct 19, 2015 - Oct 24, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS South Florida 2015 Fort Lauderdale, FL Bryan Simon	Nov 9, 2015 - Nov 14, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Sydney 2015 Sydney, Australia Dr. Eric Cole	Nov 9, 2015 - Nov 21, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS London 2015 London, United Kingdom Stephen Sims	Nov 14, 2015 - Nov 23, 2015	Register Now

FTC-0002221

Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS San Francisco 2015 San Francisco, CA Bryce Galbraith	Nov 30, 2015 - Dec 5, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Cape Town 2015 Cape Town, South Africa Dave Shackleford	Nov 30, 2015 - Dec 5, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Cyber Defense Initiative 2015 Washington, DC Paul A. Henry	Dec 12, 2015 - Dec 19, 2015	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Las Vegas 2016 Las Vegas, NV Bryce Galbraith	Jan 9, 2016 - Jan 14, 2016	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Brussels Winter 2016 Brussels, Belgium Dr. Eric Cole	Jan 18, 2016 - Jan 23, 2016	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Security East 2016 New Orleans, LA Bryan Simon	Jan 25, 2016 - Jan 30, 2016	Register Now
Training Event	Essentials	SEC401: Security Essentials Bootcamp Style SANS Munich Winter 2016 Munich, Germany Chris Christianson	Feb 15, 2016 - Feb 20, 2016	Register Now
	Essentials	SEC401: Security Essentials Bootcamp Style SANS London Spring	Feb 29, 2016 -	

FTC-0002222

Training Event		London, United Kingdom Dr. Eric Cole	Mar 5, 2016	Register Now
Summit	Essentials	SEC401: Security Essentials Bootcamp Style Cyber Defense Summit & Training Nashville, TN Dr. Eric Cole	Aug 11, 2015 - Aug 18, 2015	Register Now
Summit	Essentials	SEC401: Security Essentials Bootcamp Style Cyber Security Enforcement Summit & Training Dallas, TX Chris Christianson	Sep 21, 2015 - Sep 26, 2015	Register Now
Summit	Essentials	SEC401: Security Essentials Bootcamp Style Security Leadership Summit & Training Dallas, TX Russell Eubanks	Dec 3, 2015 - Dec 10, 2015	Register Now
Summit	Essentials	SEC401: Security Essentials Bootcamp Style Threat Hunting and Incident Response Summit New Orleans, LA Staff	Apr 12, 2016 - Apr 19, 2016	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Columbia SEC401 Columbia, MD Chris Christianson	Sep 7, 2015 - Sep 12, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Milwaukee SEC401 Milwaukee, WI Staff	Sep 14, 2015 - Sep 19, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Burnaby SEC401 Burnaby, BC Staff	Sep 21, 2015 - Sep 26, 2015	Register Now

FTC-0002223

Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Ottawa SEC401 Ottawa, ON Staff	Sep 21, 2015 - Sep 26, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Kansas City SEC401 Kansas City, MO Staff	Sep 28, 2015 - Oct 3, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Madison SEC401 Madison, WI Doc Blackburn	Oct 5, 2015 - Oct 10, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Jacksonville SEC401 Jacksonville, FL Staff	Oct 12, 2015 - Oct 17, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Rockville SEC401 Rockville, MD Staff	Oct 19, 2015 - Oct 24, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Paris SEC401 (in French) Paris, France Christophe RENARD	Oct 26, 2015 - Oct 31, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Anaheim SEC401 Anaheim, CA Staff	Oct 26, 2015 - Oct 31, 2015	Register Now
	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS New York SEC401	Nov 9, 2015 -	

FTC-0002224

Community SANS		New York, NY Doc Blackburn	Nov 14, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS San Antonio SEC401 San Antonio, TX Staff	Nov 9, 2015 - Nov 14, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Salt Lake City SEC401 Salt Lake City, UT Staff	Nov 16, 2015 - Nov 21, 2015	Register Now
Community SANS	Essentials	SEC401: Security Essentials Bootcamp Style Community SANS Toronto SEC401 Toronto, ON Staff	Dec 7, 2015 - Dec 12, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Chantilly, VA Patrick Ouellette	Jul 20, 2015 - Sep 28, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Singapore, Singapore Yee Ching Tok	Aug 14, 2015 - Oct 16, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Raleigh, NC Allen Hadder	Aug 20, 2015 - Oct 22, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Charleston, SC Janice Pryor	Sep 17, 2015 - Nov 19, 2015	Register Now

FTC-0002225

Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session San Antonio, TX James Hart	Oct 6, 2015 - Dec 8, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Downers Grove, IL Ramesh Krishnan	Oct 8, 2015 - Dec 17, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Philadelphia, PA Greg Scheidel	Oct 12, 2015 - Nov 23, 2015	Register Now
Mentor	Essentials	SEC401: Security Essentials Bootcamp Style Mentor Session Brentwood, TN Justin Bumpus	Oct 14, 2015 - Dec 16, 2015	Register Now
vLive	Essentials	SEC401: Security Essentials Bootcamp Style Online Tanya Baccam	Sep 1, 2015 - Oct 8, 2015	Register Now
vLive	Essentials	SEC401: Security Essentials Bootcamp Style Online Russell Eubanks	Nov 2, 2015 - Dec 9, 2015	Register Now
OnDemand	Essentials	SEC401: Security Essentials Bootcamp Style Online —	Anytime	Register Now
Simulcast	Essentials	SEC401: Security Essentials Bootcamp Style Online Dr. Eric Cole	Aug 13, 2015 - Aug 18, 2015	Register Now

FTC-0002226

Simulcast	Essentials	SEC401: Security Essentials Bootcamp Style Online Dr. Eric Cole	Sep 14, 2015 - Sep 19, 2015	Register Now
Simulcast	Essentials	SEC401: Security Essentials Bootcamp Style Online Paul A. Henry	Dec 14, 2015 - Dec 19, 2015	Register Now
SelfStudy	Essentials	SEC401: Security Essentials Bootcamp Style Online —	Anytime	Register Now
Private Training	All	Private Training Course of Your Choice	Your Choice	Learn More

Course contents may vary depending upon location, see specific event description for details.

Latest Whitepapers

Psychology and the hacker - Psychological Incident Handling
By Sean Atkinson

A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains
By Babu Veerappa Srinivas

A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5 Process Assessment Model (PAM)
By Muzamil Riffat

Last 25 Papers »

Latest Tweets @SANSInstitute

Hear how not to fail at cyber defense w/ Mark Burnette @lbmc [...]
July 9, 2015 - 6:10 PM

SANS Cyber Security Training in Virginia Beach including 13 [...]
July 9, 2015 - 4:56 PM

LAS VEGAS! Learn WEB APP Penetration Testing w/ @sethmisenar [...]
July 9, 2015 - 3:15 PM

Contact Us

301-654-SANS(7267)
Mon-Fri 9am - 8pm EST/EDT
info@sans.org

"As a security professional, this info is foundational to do a competent job, let alone be successful."
- Michael Foster, Providence Health and Security

"SANS is a great place to enhance your technical and hands-on skills and tools. I thoroughly recommend it."
- Aaron Waugh, Datacom NZ Ltd

"SANS always provides you what you need to become a better security professional at the right price."
- Rasik Vekaria, BP

FTC-0002227

Find Training | Live Training | Online Training | Programs | Resources | Vendor | About
Privacy Policy | Trademark Usage Policy | Credits | © 2000-2015 SANS™ Institute

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 4
TO EXPERT REPORT OF DR. ERIC B. COLE

Trust the CLOUD for sensitive info? Take Survey & Enter to Win $400 Amazon Card

SEC501: Advanced Security Essentials - Enterprise Defender

Contents | Additional Info

Delivery Methods:
Live | Online

GCED Certification
Affiliate Pricing
36 CPEs
Laptop Required

For an intensive and in-depth course, I found SEC501 to be extremely educational yet fun and entertaining.
Hisham Al-Muhareb, Saudi Aramco

Best class I've ever taken. Instructor has far more real-world experience than instructor from global knowledge with whom I've taken many classes.
Bruce Henkel, Harris Corporation

Effective cybersecurity is more important than ever as attacks become stealthier, have a greater financial impact, and cause broad reputational damage. SEC501: Advanced Security Essentials - Enterprise Defender builds on a solid foundation of core policies and practices to enable security teams to defend their enterprise.

It has been said of security that "prevention is ideal, but detection is a must." However, detection without response has little value. Network security needs to be constantly improved to prevent as many attacks as possible and to swiftly detect and respond appropriately to any breach that does occur. This PREVENT - DETECT - RESPONSE strategy must be in place both externally and internally. As data become more portable and networks continue to be porous, there needs to be an increased focus on data protection. Critical information must be secured regardless of whether it resides on a server, in a robust network architecture, or on a portable device.

Of course, despite an organization's best efforts to prevent network attacks and protect its critical data, some attacks will still be successful. Therefore, organizations need to be able to detect attacks in a timely fashion. This is accomplished by understanding the traffic that is flowing on your networks, looking for indications of an attack, and performing penetration testing and vulnerability analysis against your organization to identify problems and issues before a compromise occurs.

Finally, once an attack is detected we must react quickly and effectively and perform the forensics required. Knowledge gained by understanding how the attacker broke in can be fed back into more effective and robust preventive and detective measures, completing the security lifecycle.

Get Registered

Free Excerpt

Course List

Curricula

Share

g+1 Tweet Like

SANS

SEC401: Security Essentials Bootcamp Style

Learn to Build a Security Roadmap that can Scale Today & into the Future

LEARN MORE

FTC-0002229

More

Course Syllabus

Collapse All

Course Contents

SEC501.1: Defensive Network Infrastructure

Overview

Making your network secure from attack starts with designing, building, and implementing a robust network infrastructure. There are many aspects to implementing a defense-in-depth network that are often overlooked when companies focus only on functionality. Achieving the proper balance between business drivers and core information security requires that an organization build a secure network that is mission-resilient to a variety of potential attacks.

On the first course day students will learn how to design and build a secure network that can both prevent attacks and recover after a compromise. They will also learn how to retrofit an existing network to achieve the level of protection that is required. Building a network is not that complicated, but it takes special skills to integrate all of the components so the network can withstand a variety of attacks and support the organization's mission. Students will learn how to design and implement a functionality-rich, secure network and how to maintain and update it as the threat landscape evolves.

CPE/CMU Credits: 6

Topics

- Introduction to network security infrastructure as the target for attacks
- Impact of compromised routers and switches
- Escalating privileges at Layers 2 and 3
- Weaknesses in Cisco router and switch architecture
- Integrating and understanding existing network devices to defend against attacks
- Implementing the Cisco Gold Standard to improve security
- CISecurity Levels 1 and 2 benchmarks for routers
- SANS Gold Standard switch configuration
- Implementing security on an existing network and rolling out new devices
- Advanced Layer 2 and 3 Controls
- Filtering with access control lists
- DHCP, ARP snooping, and port security
- Introduction to network admission control and 802.1x

SEC501.2: Packet Analysis

Overview

"Prevention is ideal, but detection is a must" is a critical motto for network security professionals. While organizations always want to prevent as many attacks as possible, some adversaries will

Topics

- Architecture design and preparing filters
- Building intrusion detection capability into a network
- Understanding the components currently in

FTC-0002230

still sneak into the network. In cases where an attack cannot be prevented, security professionals must detect the indications that the attack is in progress and stop it before significant harm is caused. Packet analysis and intrusion detection are at the core of such timely detection. Organizations need to not only detect attacks but also to react in a way that ensures those attacks can be prevented in the future.

Because of the changing landscape of attacks, detecting them is an ongoing challenge. Today's attacks are more stealthy and difficult to find than ever before. Only by understanding the core principles of traffic analysis can you become a skilled analyst able to differentiate between normal and attack traffic. New attacks are surfacing all the time, so security professionals must be able to write rules that detect the latest advanced zero-day attacks before they compromise a network.

Traffic analysis and intrusion detection used to be treated as a separate discipline within many organizations. Today, prevention, detection, and reaction must be closely knit so that once an attack is detected, defensive measures can be adapted, proactive forensics implemented, and the organization can to continue to operate.

CPE/CMU Credits: 6

place

- Detection techniques and measures
- Understanding various types of traffic occurring on a network
- Knowing how normal traffic works
- Differentiating between attacks and normal users on a network
- Advanced IP packet analysis
- Performing deep packet inspection and understanding usage of key fields
- Event correlation and analysis
- Analyzing an entire network instead of a single device
- Building advanced snort rules
- Intrusion detection tools
- Installing and using analysis software
- Wireshark
- Building custom filters

SEC501.3: Pentest

Overview

Security is all about understanding, mitigating, and controlling the risk to an organization's critical assets. An organization must understand the changing threat landscape and have the capacity to compare it against its own vulnerabilities that could be exploited to compromise its network. While this was never an easy task, it is becoming much more difficult because threats are evolving rapidly and organizations are so complex. On day three, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration testing.

Finding basic vulnerabilities is easy but not necessarily effective if these are not the vulnerabilities attackers exploit to break into a

Topics

- Variety of penetration testing methods
- Frequency and use of vulnerability analysis, penetration testing, and security assessment
- Vulnerability analysis
- How to perform vulnerability analysis
- Key areas to identify and ways to fix potential problems
- Key tools and techniques
- Tools, techniques, and methods used in testing
- Basic penetration testing
- Methods and means of performing a penetration test
- Focus, requirements, and outputs of a successful test
- Prioritizing and remediation of issues
- Advanced penetration testing

FTC-0002231

system. Advanced penetration testing involves understanding the variety of systems and applications on a network and how they can be compromised by an attacker. Students will learn about both external and internal penetration testing and the methods of black, gray, and white box testing.

Penetration testing is critical to identify an organization's exposure points, but students will also learn how to prioritize and fix these vulnerabilities to increase the organization's overall security.

CPE/CMU Credits: 6

- Understanding and mapping to an organization's infrastructure
- Application testing and system analysis

SEC501.4: First Responder

Overview

Any organization connected to the Internet or that has employees is going to have attacks launched against it. Even with a keen focus on robust network design, preventive security, and identifying vulnerabilities through penetration testing, some attacks will still occur. In these cases, identifying, analyzing, and responding effectively to the attack is critical.

Security professionals need to understand how to perform incident response, analyze what is occurring, and restore their organization back to its normal state as soon as possible. Day four will provide students with a proven six-step process to follow in response to an attack: Prepare, Identify, Contain, Eradicate, Recover, and Learn from previous incidents. Cyber incidents are a lot like a fire-the sooner you detect them, the easier they are to contain, and the less damage they cause. Therefore prompt incident response is a key follow-on to intrusion analysis.

Another key aspect of incident response is forensic analysis and discovery. Students will learn how to perform forensic investigation and identify indications of an attack. This information will be fed into the incident response process to ensure that the attack is prevented from occurring again in the future.

CPE/CMU Credits: 6

Topics

- Incident handling process and analysis
- Preparing for an incident
- Identifying and responding
- Containing a problem to preserve mission resilience
- Identifying and eradicating the problem
- Recovery system data, including restoring to normal operation
- Lessons learned and follow-up reporting
- Forensics and incident response
- Windows response skills
- Windows forensics tool chest
- Linux/Unix response and analysis
- Linux/Unix tools and system analysis

SEC501.5: Malware

Overview

As security professionals continue to build more proactive security measures, the methods of attackers will continue to evolve. A common way for attackers to target, control, and break into as many systems as possible is through the use of malware. Students must therefore understand what type of malware is currently available to attackers, as well as future trends and methods of exploiting systems. With this knowledge, students can then learn how to analyze, defend, and detect malware on systems and minimize its impact on the organization.

CPE/CMU Credits: 6

Topics

- Malware
- Types of malware and corresponding behavior
- Dealing with malware
- Tying malware into intrusion analysis and incident response
- Windows malware
- Using Microsoft Windows basic built-in CLI tools
- Using Microsoft Windows advanced built-in CLI tools
- Using Microsoft Windows built-in GUI tools
- External tools and analysis
- Using external tools to fight BHO
- Fighting rootkits with basic and advanced tools
- Inspecting active processes
- Using online resources to get help

SEC501.6: Data Loss Prevention

Overview

Cybersecurity is all about managing, controlling, and mitigating risk to your critical assets. In almost every organization, critical assets are made up of data or information. Whether it is a customer list, research plans, intellectual property, classified information, or a marketing plan, these data represent your organization's lifeline and must be properly protected. Perimeters are still important and critical, but as our networks become more porous and our data more portable, we are moving away from a fortress model and moving towards a focus on data.

Information no longer solely resides on servers where properly configured access control lists can limit access and protect our information. The same intellectual property that is protected on a server behind a strong perimeter can now be copied to laptops (i.e., portable servers) and plugged into networks (i.e., hotels, airports, and coffee shops). Those venues have no firewalls or security devices in place. This means that you must be able to protect the data no matter where

Topics

- Risk management
- Calculating and understanding risk across an organization
- Building proper risk mitigation plans
- Applying proactive risk management processes
- Incorporating risk management into all business processes
- Understanding insider threats
- Data classification
- Building a data classification program
- Key aspects of deploying and implementing classification of critical information
- Staged roll-out of classifying new and existing information
- Managing and maintaining portable data classification
- Digital rights management
- Understanding digital rights
- Balancing digital rights with data classification
- Managing access across the enterprise
- Balancing functionality and security
- Data loss prevention (DLP)
- Identifying requirements and goals for

it resides. A compromise of sensitive data will have an impact on your company-no matter how or where it was stolen.

Building a strong perimeter defense is a critical first step, but focusing on protecting and controlling critical data from loss is also critical to building strong preventive measures. Proactive security must be implemented to properly protect critical information and minimize its exposure.

CPE/CMU Credits: 6

preventing data loss
- Identifying practical DLP solutions that work
- Managing, evaluating, implementing, and deploying DLP

Additional Information

Testimonial

"This is the best technical training course I have ever taken. SEC501 exposed me to many valuable concepts and tools but also gave me a solid introduction to those tools so that I can continue to study and improve on my own." - *Curt Smith, Hildago Medical Services*

"SEC501 offers a great explanation of Net Defense best practices that often get overlooked." - *Kirk G., U.S. Navy*

"For an intensive and in-depth course, I found SEC501 to be extremely educational yet fun and entertaining." -*Hisham Al-Muhareb, Saudi Aramco*

Laptop Required

A properly configured laptop is required to participate in SEC501: Advanced Security Essentials - Enterprise Defender. Students must have Administrator privileges. Antivirus software is not recommended and may need to be disabled or uninstalled. If you have a production system already installed with data on it that you do not want to lose, it is recommended that you replace it with a clean hard drive.

Prior to the start of class, you must install the necessary software as described below. The following are minimal hardware requirements for your laptop:

- DVD-RW drive
- 4 GB RAM (more memory is strongly recommended)
- 40GB of available disk space (more space is recommended)
- 4GB USB memory stick
- Windows 7 32-bit virtual machine

Please note: Windows 7 32-bit and VMWare Workstation is an explicit requirement for SEC501.

You will use VMware to simultaneously run multiple virtual machines when performing hands-on

exercises. You must have VMware Workstation installed on your system. If you do not own VMware, you can download a free 30-day trial copy from the VMware website. If taking advantage of the trial offer, please make sure that the license will not expire before you complete the course. You will also need WinRAR installed.

While most labs will run fine for MAC/Fusion students, this configuration has not been tested and is not supported.

Final Checklist

We suggest going over the following checklist to make sure that your laptop is prepared for SANS SEC501: Advanced Security Essentials - Enterprise Defender:

- The laptop meets hardware requirements outlined in this note.
- If you use a trial copy of VMware Workstation, make sure that the VMware license will not expire before the class ends.
- You created a Windows 7 32-bit virtual machine image (no latest updates from Microsoft needed).
- The Windows VMware machine runs using host-only networking mode.

If you have additional questions about the laptop specifications, please contact laptop_prep@sans.org.

Who Should Attend

- Incident response and penetration testers
- Security Operations Center engineers and analysts
- Network security professionals
- Anyone who seeks technical in-depth knowledge about implementing comprehensive security solutions

Prerequisites

While not required, it is recommended that students take SEC401: Security Essentials or have the skills taught in that class. This includes a detailed understanding of networks, protocols, and operating systems.

You Will Be Able To

- Identify network security threats against infrastructure and build defensible networks that minimize the impact of attacks
- Access tools that can be used to analyze a network to prevent attacks and detect the adversary
- Decode and analyze packets using various tools to identify anomalies and improve network defenses
- Understand how the adversary compromises systems and how to respond to attacks
- Perform penetration testing against an organization to determine vulnerabilities and points of compromise
- Apply the six-step incident handling process

- Use various tools to identify and remediate malware across your organization
- Create a data classification program and deploy data-loss-prevention solutions at both a host and network level

Hands-on Training

The students will participate in labs that:

- Analyze network configurations for routers
- Perform detailed analysis of traffic using various sniffers and protocol analyzers
- Identify and track attacks and anomalies in network packets
- Use various tools to perform penetration testing and network discovery
- Analyze both Windows and Unix systems during an incident to identify signs of a compromise
- Find, identify, and clean up various types of malware

Author Statement

After I finish teaching SEC401-the precursor to the SEC501 course-it is always a thrill to see students leave with fire in their eyes and an excitement about them. They walked into class feeling overwhelmed that security is a lost cause, but now they leave class understanding what they need to do, and they have a focus and drive to do the right thing to secure their organizations.

The next question we receive on a constant basis is, what course should I take next? How do I continue my journey? Well, it depends on your focus area. Do you want to get more into perimeter protection, IDS, operating system security, etc.? The challenge is that many students work in jobs that do not allow them to focus on one area; they need to understand all of the key areas across security.

What students are telling us is that they want a Security Essentials Part 2 or a 500-level continuation of Security Essentials covering the next level of technical knowledge. With SEC501, SANS has decided to give students just what they have been asking for. I am beyond thrilled with the results: we have identified core foundation areas that complement SEC401 with no overlap and continue to build a solid security foundation for network practitioners.

After one recent class, a student ran up and gave me a big hug (he was a retired football player, so I did not argue) and said, "SANS is awesome. I have been frustrated in my job for over a year and had lost hope that you really could secure an organization and that anything I did made a difference. Just as my light of hope was burning out, I decided to take the Security Essentials course, figuring it was a lost cause. After this class the fire is burning brighter than it ever was. I feel like a kid again and cannot wait to go back to my company and make a difference. However, I think my boss is scared because I called him eight times throughout the week, telling him all of the great information and practical knowledge I learned!"

Having taught thousands of students, I am confident you will be just as excited and get similar results from SEC501. However, just for reference, hugs are optional.

- Eric Cole

Additional Resources

Take your learning beyond the classroom. Explore our site network for additional resources related to this course's subject matter.

Cyber Defense

FTC-0002236

*CPE/CMU credits not offered for the SelfStudy delivery method

Online options available. Train from any location. OnDemand

17 Training Results

All | Training Events | Community SANS | Mentor | Virtual | Online

Type	Topic	Course / Location / Instructor	Date	Register
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Minneapolis 2015 Minneapolis, MN Keith Palmgren	Jul 20, 2015 - Jul 25, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Boston 2015 Boston, MA Keith Palmgren	Aug 3, 2015 - Aug 8, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Virginia Beach 2015 Virginia Beach, VA Dr. Eric Cole	Aug 24, 2015 - Sep 4, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Chicago 2015 Chicago, IL Bryan Simon	Aug 30, 2015 - Sep 4, 2015	Register Now
	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Network Security 2015	Sep 12, 2015 -	

FTC-0002237

Training Event		Las Vegas, NV Paul A. Henry	Sep 21, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Seattle 2015 Seattle, WA Bryan Simon	Oct 5, 2015 - Oct 10, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Tysons Corner 2015 Tysons Corner, VA Keith Palmgren	Oct 12, 2015 - Oct 17, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Cyber Defense San Diego 2015 San Diego, CA Paul A. Henry	Oct 19, 2015 - Oct 24, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Sydney 2015 Sydney, Australia Dr. Eric Cole	Nov 9, 2015 - Nov 21, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS London 2015 London, United Kingdom Paul A. Henry	Nov 14, 2015 - Nov 23, 2015	Register Now
Training Event	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender SANS Cyber Defense Initiative 2015 Washington, DC Bryan Simon	Dec 12, 2015 - Dec 19, 2015	Register Now

FTC-0002238

Summit	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender Security Awareness Summit & Training Philadelphia, PA Bryan Simon	Aug 17, 2015 - Aug 25, 2015	Register Now
Community SANS	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender Community SANS Columbia SEC501 Columbia, MD Bryan Simon	Aug 3, 2015 - Aug 8, 2015	Register Now
OnDemand	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender Online —	Anytime	Register Now
Simulcast	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender Online Paul A. Henry	Sep 14, 2015 - Sep 19, 2015	Register Now
SelfStudy	Essentials	SEC501: Advanced Security Essentials - Enterprise Defender Online —	Anytime	Register Now
Private Training	All	Private Training Course of Your Choice	Your Choice	Learn More

Course contents may vary depending upon location, see specific event description for details.

Latest Whitepapers

Psychology and the hacker - Psychological

Latest Tweets @SANSInstitute

Hear how not to fail at cyber defense w/ Mark

Contact Us

301-654-SANS(7267)

FTC-0002239

Incident Handling
By Sean Atkinson

A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains
By Babu Veerappa Srinivas

A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5 Process Assessment Model (PAM)
By Muzamil Riffat

Burnette @lbmc [...]
July 9, 2015 - 6:10 PM

SANS Cyber Security Training in Virginia Beach including 13 [...]
July 9, 2015 - 4:56 PM

LAS VEGAS! Learn WEB APP Penetration Testing w/ @sethmisenar [...]
July 9, 2015 - 3:15 PM

Last 25 Papers »

Mon-Fri 9am - 8pm EST/EDT
info@sans.org

"It was a great learning experience that helped open my eyes wider. The instructor's knowledge was fantastic."
- Manuja Wikesekera, Melbourne Cricket Club

"Just amazing content and instruction, it's really a 'must do' for any info sec professional."
- Mark Austin, PHH Mortgage

"SANS always provides you what you need to become a better security professional at the right price."
- Rasik Vekaria, BP

 © 2000-2015 SANS™ Institute

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 5
TO EXPERT REPORT OF DR. ERIC B. COLE

Trust the CLOUD for sensitive info? Take Survey & Enter to Win $400 Amazon Card

SEC566: Implementing and Auditing the Critical Security Controls - In-Depth

Contents | Additional Info

Delivery Methods:
Live | Online

GCCC Certification
Affiliate Pricing
30 CPEs
Laptop Required

Provides greater structure to the basic controls good methodology provided in implemenating controls.
Jalal Moloo, JB Shenker

Leaving the class with a great mind set for evaluating current environment and controls.
Tom Kozelsky, Nexeo Solution

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches?

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course on how to implement the Twenty Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

Get Registered

Free Excerpt

Course List

Curricula

Share

g+1 Tweet Like

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

More

Course Syllabus

Collapse All

Course Contents

SEC566.1: Introduction and Overview of the 20 Critical Controls

Overview

During day 1, we will cover an introduction and overview of the 20 Critical Controls, laying the foundation for the rest of the class. For each control the following information will be covered, and we will follow the same outline for each control:

1. Overview of the Control
2. How it is Compromised
3. Defensive Goals
4. Quick Wins
5. Visibility & Attribution
6. Configuration & Hygiene
7. Advanced
8. Overview of Evaluating the Control
9. Core Evaluation Test(s)
10. Testing/Reporting Metrics
11. Steps for Root Cause Analysis of Failures
12. Audit/Evaluation Methodologies
13. Evaluation Tools
14. Exercise to Illustrate Implementation Or Steps for Auditing a Control

In addition, Critical Controls 1 and 2 will be covered in depth.

Critical Control 1: Inventory of Authorized and Unauthorized Devices

Any time a new device is installed on a network, the risks of exposing the network to unknown vulnerabilities or hampering its operation are present. Malicious code can take advantage of new hardware that is not configured and patched with appropriate security updates at the time of installation. Attackers can use these vulnerable systems to install backdoors before they are hardened. In automating critical control 1, it's critical for all devices to have an accurate and up-to-date inventory control system in place. Any device not in the database should be prohibited from connecting to the

FTC-0002242

network. Some organizations maintain asset inventories by using specific large-scale enterprise commercial products or by using free solutions to track and sweep the network periodically. To evaluate the implementation of Control 1 on a periodic basis, the evaluation team will connect hardened test systems to at least 10 locations on the network. This will include a selection of subnets associated with DMZs, workstations, and servers.

Critical Control 2: Inventory of Authorized and Unauthorized Software

An organization without the ability to inventory and control its computer's installed programs makes its systems more vulnerable to attack. Furthermore, poorly controlled machines are more likely to be running software that is unneeded for business purposes, introducing potential security flaws. Compromised systems become a staging point for attackers to collect sensitive information. In order to combat this potential threat, an organization should scan a network and identify known or responding applications. Commercial software and asset inventory tools are widely available. The best tools provide an inventory check of hundreds of common applications, pulling information about the patch level of each installed program. This ensures that it's the latest version and that it leverages standardized application names, like those found in the Common Platform Enumeration (CPE) specification. In addition to inventory checks, tools that implement whitelists (allow) and blacklists (deny) of programs are included in many modern end-point security suites. To evaluate the implementation of Control 2 on a periodic basis, the team must move a benign software test program that is not included in the authorized software list on 10 systems on the network. The team must then verify that the software is blocked and unable to run.

CPE/CMU Credits: 6

SEC566.2: Critical Controls 3,4,5 and 6

Overview

During day 2, we will cover Critical Controls 3, 4, 5 and 6.

Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

Default configurations of software are often geared to ease-of-deployment and ease-of-use and not security, leaving some systems exploitable in their default state. Attackers attempt to exploit both network-accessible services and client software using various forms of malware. Without the ability to inventory and control installed and running, enterprises make their systems more vulnerable. Organizations can implement this control by developing a series of images and secure storage servers for hosting these standard images. Configuration management tools can be employed to measure the settings of the installed software and to look for deviations from the standard image configurations used by the organization. To evaluate the implementation of Control 3 on a periodic basis, an evaluation team must move a benign test system (one that does not contain the official hardened image, but does contain additional services, ports, and configuration files changes) onto the network. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the changes to the software.

Critical Control 4: Continuous Vulnerability Assessment and Remediation

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and launch it against targets of interest. Any significant delays finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through and gain control of vulnerable machines. A large number of vulnerability scanning tools are available to

evaluate the security configuration of systems. The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. All machines identified by the asset inventory system must be scanned for vulnerabilities. To evaluate the implementation of Control 4 on a periodic basis, the evaluation team must verify that scanning tools have successfully completed their weekly or daily scans.

Critical Control 5: Malware Defenses

Malicious software is an integral and dangerous aspect of Internet threats. It targets end users and organizations via Web browsing, e-mail attachments, mobile devices, and other vectors. Malicious code may tamper with a system's contents, capture sensitive data, and spread to other systems. To ensure anti-virus signatures are up-to-date, effective organizations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based Intrusion Detection Systems (IDS) features are active on every managed system. They also run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections or do not have the latest malware definitions. The system must identify any malicious software that is either installed, attempted to be installed, executed, or attempted to be executed, on a computer system. To evaluate the implementation of Control 5 on a periodic basis, the evaluation team must move a benign software test program appearing to be malware onto a system and make sure it is properly discovered and remediated.

Critical Control 6: Application Software Security

Criminal organizations frequently attack vulnerabilities in both web-based and non-web-based application software. In fact, it's a top priority for criminals.

Application software is vulnerable to remote compromise in three ways:

- It does not properly check the size of user input
- It fails to sanitize user input by filtering out potentially malicious character sequences
- It does not initialize and clear variables properly

To avoid attacks, internally developed and third party application software must be carefully tested to find security flaws. Source code testing tools, web application security scanning tools, and object code testing tools have proven useful in securing application software. Another useful tool is manual application security penetration testing by testers who have extensive programming knowledge and application penetration testing expertise. The system must be capable of detecting and blocking an application-level software attack, and must generate an alert or send e-mail to enterprise administrative personnel. To evaluate the implementation of Control 6 on a monthly basis, an evaluation team must use a web application vulnerability scanner to test software security flaws.

CPE/CMU Credits: 6

SEC566.3: Critical Controls 7, 8, 9, 10 and 11

Overview

During day 3, we will cover Critical Controls 7, 8, 9, 10 and 11.

Critical Control 7: Wireless Device Control

Attackers who gain wireless access to an organization from nearby parking lots have initiated major data thefts. This allows attackers to bypass an organization to maintain long-term access inside a target.

Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems. The system must be capable of identifying unauthorized wireless devices or configurations when they are within range of the organization's systems or connected to its networks. To evaluate the implementation of Control 7 on a periodic basis, the evaluation team staff must configure unauthorized but hardened wireless clients and wireless access points to the organization's network. It must also attempt to connect them to the organization's wireless networks. These access points must be detected and remediated in a timely manner.

Critical Control 8: Data Recovery Capability (validated manually)

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. Once per quarter, a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and datum from the backup are all intact and functional.

Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)

An organization hoping to find and respond to attacks effectively relies on its employees and contractors to find the gaps and fill them. A solid security skills assessment program can provide actionable information to decision makers about where security awareness needs to be improved. It can also help determine proper allocation of limited resources to improve security practices. The key to upgrading skills is measurement, not with certification examinations, but with assessments that show both the employee and the employer where knowledge is sufficient and where there are gaps. Once the gaps have been identified, those employees who have the requisite knowledge can be called upon to mentor the employees who do not. The organization can also develop training programs that directly maintain employee readiness.

Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Attackers penetrate defenses by searching for electronic holes in firewalls, routers, and switches. Once these network devices have been exploited, attackers can gain access to target networks, redirect traffic on that network (to a malicious system masquerading as a trusted system), and intercept and alter information while in transmission. Organizations can use commercial tools that will evaluate the rule set of network filtering devices, which determine whether they are consistent or in conflict and provide an automated check of network filters. Additionally, these commercial tools search for errors in rule sets. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies. To evaluate the implementation of Control 10 on a periodic basis, an evaluation team must make a change to each type of network device plugged into the network. At a minimum, routers, switches, and firewalls need to be tested. If they exist, IPS, IDS, and other network devices must be included.

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

Attackers search for remotely accessible network services that are vulnerable to exploitation. Many software packages automatically install services and turn them on as part of the installation of the main software package. When this occurs, the software rarely informs a user that the services have been enabled. Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port. The system must be capable of identifying any new unauthorized listening network ports that are connected to the network. To evaluate the implementation of Control 11 on a periodic basis, the evaluation team must install hardened test services with network listeners on ten locations on the network, including a selection of subnets associated with DMZs, workstations, and servers.

CPE/CMU Credits: 6

SEC566.4: Critical Controls 12, 13, 14 and 15

Overview

During day 4, we will cover Critical Controls 12, 13, 14 and 15.

Critical Control 12: Controlled Use of Administrative Privileges

The most common method attackers use to infiltrate a target enterprise is through an employee's own misuse of administrator privileges. An attacker can easily convince a workstation user to open a malicious e-mail attachment, download and open a file from a malicious site, or surf to a site that automatically downloads malicious content. If the user is logged in as an administrator, the attacker has full access to the system. Built-in operating system features can extract lists of accounts with superuser privileges, both locally on individual systems and on overall domain controllers. These accounts should be monitored and tracked very closely. To evaluate the implementation of Control 12 on a periodic basis, an evaluation team must verify that the organization's password policy is enforced and administrator accounts are carefully controlled. The evaluation team does this by creating a temporary, disabled, limited privilege test account on ten different systems. It then attempts to change the password on the account to a value that does not meet the organization's password policy.

Critical Control 13: Boundary Defense

By attacking Internet-facing systems, attackers can create a relay point to break into other networks or internal systems. Automated tools can be used to exploit vulnerable entry points into a network. To control the flow of traffic through network borders and to look for attacks and evidence of compromised machines, boundary defenses should be multi-layered. These boundaries should consist of firewalls, proxies, DMZ perimeter networks, and network-based intrusion prevention systems and intrusion detection systems. Organizations should regularly test these sensors by launching vulnerability-scanning tools. These tools verify that the scanner traffic triggers an appropriate alert. The captured packets of the Intrusion Detection Systems (IDS) sensors should be reviewed using an automated script each day, which ensures log volumes are within expected parameters, are formatted properly, and have not been corrupted. To evaluate the implementation of Control 13 on a periodic basis, an evaluation team must test boundary devices. This is done by sending packets from outside a trusted network, which ensures that only authorized packets are allowed through the boundary. All other packets must be dropped.

Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs

At times, audit logs provide the only evidence of a successful attack. Many organizations keep audit records for compliance purposes but rarely review them. When audit logs aren't reviewed, organizations don't know their systems have been compromised. Attackers rely on this. Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, and logs should be sent to centralized logging servers. The system must be capable of logging all events across the network. The logging must be validated across both network and host-based systems. To evaluate the implementation of Control 14 on a periodic basis, an evaluation team must review the security logs of various network devices, servers, and hosts.

Critical Control 15: Controlled Access Based On Need to Know

Some organizations do not carefully identify and separate sensitive data from less sensitive, publicly available information within an internal network. In many environments, internal users have access to all or most of the information on the network. Once attackers have penetrated such a network, they can easily find and exfiltrate important information with little resistance. This control is often implemented

using the built-in separation of administrator accounts from non-administrator accounts. The system must be able to detect all attempts by users to access files without the appropriate privileges and must generate an alert or e-mail for administrative personnel. This includes information on local systems or network accessible file shares. To evaluate the implementation of Control 15 on a periodic basis, the evaluation team must create test accounts with limited access and verify that the account is unable to access controlled information.

CPE/CMU Credits: 6

SEC566.5: Critical Controls 16, 17, 18, 19 and 20

Overview

During day 5, we will cover Critical Controls 16, 17, 18, 19 and 20.

Critical Control 16: Account Monitoring and Control

Attackers frequently impersonate legitimate users through inactive user accounts. This method makes it difficult for network watchers to identify attackers' behavior. Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Security personnel can configure systems to record more detailed information about account access and utilize homegrown scripts or third-party log analysis tools to analyze this information. The system must be capable of identifying unauthorized user accounts when they exist on the system. To evaluate the implementation of Control 16 on a periodic basis, the evaluation team must verify that the list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire has successfully been completed daily.

Critical Control 17: Data Loss Prevention

The loss of protected and sensitive data is a serious threat to business operations, and potentially, national security. While some data is leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices. These include, but are not limited to, a lack of effective policy architectures and user error. The phrase "Data Loss Prevention" (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Commercial DLP solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. The system must be capable of identifying unauthorized datum leaving the organization's systems whether via network file transfers or removable media. To evaluate the implementation of Control 17 on a periodic basis, the evaluation team must attempt to move test datum sets (that trigger DLP systems but do not contain sensitive data) outside of the trusted computing environment via both network file transfers and via removable media.

Critical Control 18: Incident Response Capability (validated manually)

Without an incident response plan, an organization may not discover an attack in the first place. Even if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have far higher impact on the target organization, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible. After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training. This includes, but is not limited to, working through a series of attack scenarios that are fine-tuned to the threats and

vulnerabilities the organization faces.

Critical Control 19: Secure Network Engineering (validated manually)

Security controls can be circumvented in networks that are poorly designed. Without carefully planned and properly implemented network architecture, attackers can pivot through the network to gain access to target machines. To help ensure a consistent, defensible network, the architecture of each network should be based on a template that describes the overall layout of the network and the services it provides. Organizations should prepare network diagrams for each of their networks. Network diagrams should show components such as routers, firewalls, switches, significant servers, and groups of client machines.

Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Penetration testing involves mimicking the actions of computer attackers, and exploiting them to determine what kind of access an attacker can gain. Each organization should define a clear scope and the rules of engagement for penetration testing and red team analyses. The scope of such projects should include, at least, systems with the highest value information and production processing functionality.

CPE/CMU Credits: 6

Additional Information

☐ Laptop Required

SANS courses consist of instruction and hands-on sessions. The hands-on sessions are designed to allow students to utilize the knowledge gained throughout the course in an instructor-led environment. Students will have the opportunity to install, configure, and use the tools and techniques that they have learned. USB drives will be provided that will contain all of the tools required for the exercises, therefore the student's computer should have the ability to open and execute files from a USB drive.

NOTE: Please test to make sure that the computer you bring to class is not blocked from using USB disks. Lab files will only be distributed to students via USB drives in class.

Students attending this course are required to bring their own computers that are properly configured. There is not enough time in class to help you install your computer. Please note that your computer must be properly installed and configured before you come to class.

NOTE: Do not bring a regular production computer for this class! When installing software, there is always a chance of breaking something else on the system. Students should assume that all data could be lost.

NOTE: It is critical that students have administrator access to the operating system and all security software installed. This includes access to the computer's BIOS settings. If the student's computer's BIOS is password protected, they will need to have access to that password during class.

NOTE: Changes will likely need to be made to personal firewalls and other host-based software in order for the labs to work. Any anti-malware software may need to be disabled in order to install some of the tools. Therefore students must also be able to disable any anti-malware software and have the specific anti-malware software administrator passwords prior to coming to class.

RECOMMENDATION: For maximum flexibility, students can run both Microsoft Windows and Linux operating systems under virtual machines as long as the hardware on the computer can support this. The host operating system can be Windows, Linux, or Apple OSX, as long as it supports to most recent version of VMware software (Player, Workstation, or Fusion depending on the OS).

Bring a computer loaded with Microsoft Windows 7 or later with VMware Player (or similar VMWare product) loaded. Virtual box is generally not recommended for class. In either case the computer a student brings to class must support virtualization in the computer's BIOS. The Windows installation should be a default installation of the operating system with all of the options loaded. This system should be up to date on operating system patches prior to coming to class, including all updates for the .NET Framework and Microsoft Windows PowerShell. Either 32-bit or 64-bit systems will work fine for class, but the student should know which version of the operating system they have with them.

For the Linux portion of the exercises, Linux can be run from VMware image that will be provided in class. VMware can be downloaded/purchased from the VMware website. For students bringing a computer with Microsoft Windows as the host operating system, they may either choose to download the latest version of the free VMware Player software or bring the latest version of VMware Workstation (9.x or later). For students bringing a computer with Apple OSX as the host operating system, they should download and install the latest version of VMware Fusion instead.

Your computer should also have a properly configured 802.11 wireless card that works only under the host operating system, and Ethernet NIC (network interface card). In addition, the system should have a minimum of 2GB of hardware RAM, but the more RAM that is available, the easier it will be for students to complete the hands-on exercises. Prior to coming to class, the network interfaces should be tested to prove that they can be configured and that all of the proper drivers have been installed.

If you have additional questions about the laptop specifications, please contact laptop_prep@sans.org.

Who Should Attend

Who Should Attend:

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

- Alumni of

  - SEC/AUD 440: 20 Critical Security Controls: Planning, Implementing and Auditing
  - SEC401: SANS Security Essentials Bootcamp Style
  - SEC501: Advanced Security Essentials - Enterprise Defender
  - MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™
  - Other SANS Audit courses

FTC-0002249

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stop- ping known attacks and protecting organizations' important information and systems
- Understand the importance of each control, how it is compromised if ignored, and explain the defesive goals that result in quick wins and increased visibility of network and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each controls the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how critical controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the critical security controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Author Statement

As we've had the opportunity to talk with information assurance engineers, auditors, and managers over the past ten years, we've seen frustration in the eyes of these hardworking individuals who are trying to make a difference in their organizations by better defending their data systems. It has even come to the point where some organizations have decided that it's simply too hard to protect their information, and many have started to wonder, is the fight really worth it? Will we ever succeed? We see companies and agencies making headway, but the offense keeps pushing. The goal of this course is to give direction and a realistic hope to organizations attempting to secure their systems.

The 20 Critical Security Controls: Planning, Implementing, and Auditing offers direction and guidance from those in the industry who think through the eyes of the attacker as to what security controls will make the most impact. What better way to play defense than by understanding the mindset of the offense? By implementing our defense methodically and with the mindset of a hacker, we think organizations have a chance to succeed in this fight. We hope this course helps turn the tide.

- Eric Cole, Ph.D. and James Tarala

Additional Resources

Take your learning beyond the classroom. Explore our site network for additional resources related to this course's subject matter.

Audit Cyber Defense

**CPE/CMU credits not offered for the SelfStudy delivery method*

Online options available. Train from any location. OnDemand

FTC-0002250

12 Training Results

All | Training Events | Community SANS | Mentor | Virtual | Online

Type	Topic	Course / Location / Instructor	Date	Register
Training Event	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth SANS Crystal City 2015 Crystal City, VA Randy Marchany	Sep 8, 2015 - Sep 13, 2015	Register Now
Training Event	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth SANS Network Security 2015 Las Vegas, NV James Tarala	Sep 12, 2015 - Sep 21, 2015	Register Now
Training Event	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth SANS Cyber Defense Initiative 2015 Washington, DC James Tarala	Dec 12, 2015 - Dec 19, 2015	Register Now
Training Event	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth SANS Security East 2016 New Orleans, LA James Tarala	Jan 25, 2016 - Jan 30, 2016	Register Now
Summit	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Cyber Defense Summit & Training Nashville, TN Randy Marchany	Aug 11, 2015 - Aug 18, 2015	Register Now
Summit	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Security Awareness Summit & Training Philadelphia, PA Jason Fossen	Aug 17, 2015 - Aug 25, 2015	Register Now

FTC-0002251

Community SANS	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Community SANS New York SEC566 New York, NY Kenton Smith	Oct 5, 2015 - Oct 9, 2015	Register Now
Community SANS	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Community SANS Herndon-Reston SEC566 Herndon, VA Kenton Smith	Nov 16, 2015 - Nov 20, 2015	Register Now
OnDemand	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Online —	Anytime	Register Now
Simulcast	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Online Randy Marchany	Aug 13, 2015 - Aug 17, 2015	Register Now
SelfStudy	Audit IT	SEC566: Implementing and Auditing the Critical Security Controls - In-Depth Online —	Anytime	Register Now
Private Training	All	Private Training Course of Your Choice	Your Choice	Learn More

Course contents may vary depending upon location, see specific event description for details.

Latest Whitepapers Latest Tweets @SANSInstitute Contact Us

FTC-0002252

Psychology and the hacker - Psychological Incident Handling
By Sean Atkinson

A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains
By Babu Veerappa Srinivas

A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5 Process Assessment Model (PAM)
By Muzamil Riffat

Hear how not to fail at cyber defense w/ Mark Burnette @lbmc [...]
July 9, 2015 - 6:10 PM

SANS Cyber Security Training in Virginia Beach including 13 [...]
July 9, 2015 - 4:56 PM

LAS VEGAS! Learn WEB APP Penetration Testing w/ @sethmisenar [...]
July 9, 2015 - 3:15 PM

301-654-SANS(7267)
Mon-Fri 9am - 8pm EST/EDT
info@sans.org

Last 25 Papers »

"As a security professional, this info is foundational to do a competent job, let alone be successful."
- Michael Foster, Providence Health and Security

"This has been a great way to get working knowledge that would have taken years of experience to learn."
- Josh Carlson, Nelnet

"Expertise of the trainer is impressive, real life situations explained, very good manuals. Best training ever!"
- Jerry Robles de Medina, Godo CU

 © 2000-2015 SANS™ Institute

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 6
TO EXPERT REPORT OF DR. ERIC B. COLE

Critical Controls for Effective Cyber Defense

Table of Contents

Introduction: Critical Controls for Effective Cyber Defense 3

The Goal 3
The Methodology 3
Why The Controls Work 3
How to Apply the Controls 4
Prioritizing the Controls 4
Contributors 5
The Critical Controls Document 5
Moving Ahead 5

Description of Controls 6

Critical Control 1: Inventory of Authorized and Unauthorized Devices 6
Critical Control 2: Inventory of Authorized and Unauthorized Software 12
Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers 166
Critical Control 4: Continuous Vulnerability Assessment and Remediation 221
Critical Control 5: Malware Defenses 27
Critical Control 6: Application Software Security 31
Critical Control 7: Wireless Device Control 35
Critical Control 8: Data Recovery Capability 39
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps 41
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches 44
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services 48
Critical Control 12: Controlled Use of Administrative Privileges 51
Critical Control 13: Boundary Defense 55
Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs 60
Critical Control 15: Controlled Access Based on the Need to Know 64
Critical Control 16: Account Monitoring and Control 67
Critical Control 17: Data Loss Prevention 71
Critical Control 18: Incident Response and Management 75
Critical Control 19: Secure Network Engineering 78
Critical Control 20: Penetration Tests and Red Team Exercises 80

Summary and Action Plan **84**

Appendix A: Mapping between the Critical Security Controls and National Institute of Standards and Technology Special Publication 800-53, Revision 3, Priority 1 Items **85**

Appendix B: Attack Types **87**

FTC-0002255

Introduction

Critical Controls for Effective Cyber Defense

Version 4.0

To secure organizations from cyber attacks, networks and systems must vigorously defend against a variety of internal and external threats. Defenses must also be prepared to detect and thwart follow-on attacks inside a network that has already been compromised. Two guiding principles are: "Prevention is ideal but detection is a must" and "Offense informs defense."

The Goal

The goal of the Critical Controls is to strengthen the defensive posture of your organization's information security; reduce compromises, recovery efforts, and associated costs; and protect critical assets and infrastructure. The Controls provide continuous, automated monitoring of the riskiest portions of your information technology infrastructure. Having them in place will allow your organization to focus on its primary mission.

The Methodology

The Critical Controls provide a prioritized, risk-based approach to security based on actual threats. The Controls focus on automation to provide cost efficiency, measurable results, scalability, and reliability. The four critical tenets of an effective cyber defense system as reflected in the Critical Controls are:

- Offense Informs Defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective defenses.
- Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- Continuous monitoring: Carry out continuous monitoring/auditing to test and validate whether current security measures are proactively remediating vulnerabilities in a timely manner.
- Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

Why the Controls Work

The Critical Controls draw on the knowledge gained in combating the myriad attacks launched regularly against networks. Top cybersecurity experts have joined forces to make the Controls the most effective and specific set of technical measures available to detect and prevent the most common and damaging of those computer attacks. This consensus process is the foundation of the Controls because it provides first-hand knowledge of actual attacks and the best defensive

FTC-0002256

techniques to stop them. It also ensures that the Controls will address the root causes of attacks so that security measures deployed today will be effective against the next generation of advanced threats.

The Critical Controls represent the sum total of efforts over the last decade to develop standards to identify common vulnerabilities and their severity, define secure configurations, inventory systems and platforms, and pinpoint application weaknesses. These efforts include the Associated Manageable Network Plan Milestones and Network Security Tasks developed by the National Security Agency (NSA), and the Security Content Automation Program sponsored by the National Institute of Standards and Technology (NIST).

How to Apply the Controls

The Critical Controls are specific guidelines that CISOs, CIOs, IGs, and various computer emergency response teams can provide to their technical system administration and information security personnel to ensure that their systems have the most critical baseline controls in place. To help organizations with different levels of information security capabilities design a sound security baseline and then improve beyond that, the sub-controls included in each of the Critical Control summaries specify actions that organizations can take to improve their defenses:

- *Quick wins* on fundamental aspects of information security to help an organization rapidly improve its security stance without major procedural, architectural, or technical changes to its environment.
- *Visibility and attribution measures* to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.
- *Improved information security configuration and hygiene* to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.
- *Advanced sub-controls* that use new technologies that provide maximum security but are harder to deploy or more expensive than commoditized security solutions.

Prioritizing the Controls

As a result of the rigorous process of analysis, debate, and consensus that is the basis of their design, the Critical Controls are categorized by their attack migration impact and their importance in providing a direct defense against attacks. The rankings can be tailored to the cybersecurity needs and capabilities of a particular organization. Priority is given to Controls that (1) mitigate known attacks, (2) address a wide variety of attacks, and (3) identify and stop attacks early in the compromise cycle.

Contributors

The strength of the Critical Controls is in the many organizations that contributed input to identifying and designing them. These include the U.S. Departments of Defense and Energy, the U.S. Computer Emergency Readiness Team, the FBI and other law enforcement agencies, and civilian penetration testers.

The Critical Controls Document

The presentation of each Critical Control in this document includes:

- A step-by-step breakdown of the procedures and tools required to implement and automate it;
- An explanation of how attackers exploit the absence of this control;
- Entity relationship diagrams to show how the controls can be implemented;
- An outline of the most appropriate sub-controls to implement, automate, and measure effectiveness;
- Summaries of metrics and tests that can be used to evaluate implementation; and
- A list of associated NIST controls and NSA tasks.

After organizations implement the Controls and gain experience with automation, CIOs can use the document as an audit guide to ensure that they are taking the right actions for effective cyber defense, and IGs can use it to verify the CIOs' tests.

The Controls are meant to deal with multiple kinds of computer attackers, including malicious internal employees and contractors, independent individual external actors, organized crime groups, terrorists, and nation-state actors, as well as mixes of these different threats. The Controls are not limited to blocking the initial compromise of systems, but also to detecting already-compromised machines and preventing or disrupting an attacker's actions. The defenses identified through these controls deal with reducing the initial attack surface by hardening security, identifying compromised machines to address long-term threats inside an organization's network, controlling super-user privileges on systems, and disrupting attackers' command-and-control of implanted malicious code.

Finally, each control included in this document describes a series of tests that organizations can conduct on a periodic or continual basis to ensure that appropriate defenses are in place.

Moving Ahead

The consensus effort to define critical security controls is an evolving process. Changing technology and attack patterns will necessitate future changes to the current set of Critical Controls. In a sense, this will be a living document moving forward, but the Controls described here are a solid start toward making fundamental computer security defenses a well-understood, replicable, measurable, scalable, and reliable process.

FTC-0002258

Description of Controls

Critical Control 1: Inventory of Authorized and Unauthorized Devices

The processes and tools used to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.

How Do Attackers Exploit the Absence of this Control?

Many criminal groups and nation-states deploy systems that continuously scan address spaces of target organizations, waiting for new and unprotected systems to be attached to the network. The attackers also look for laptops not up to date with patches because they are not frequently connected to the network. One common attack takes advantage of new hardware that is installed on the network one evening and not configured and patched with appropriate security updates until the following day. Attackers from anywhere in the world may quickly find and exploit such systems that are accessible via the Internet. Furthermore, even for internal network systems, attackers who have already gained internal access may hunt for and compromise additional improperly secured internal computer systems. Some attackers use the local nighttime window to install backdoors on the systems before they are hardened.

APTs (advanced persistent threat) target internal users with the goal of compromising a system on the private network that can be used as a pivot point to attack internal systems. Even systems that are connected to the private network, without visibility from the Internet, can still be a target of the advanced adversary. Any system, even test systems that are connected for a short period of time, can still be used as a relay point to cause damage to an organization.

As new technology continues to come out, BYOD (bring your own device)— where employees bring personal devices into work and connect them to the network—is becoming very common. These devices could already be compromised and be used to infect internal resources.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins*: Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to an organization's public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
2. *Quick wins:* Deploy DHCP Server logging, and utilize a system to improve the asset inventory and help detect unknown systems through this DHCP information.
3. *Quick wins:* All equipment acquisitions should automatically update the inventory system as new, approved devices are connected to the network. A robust change control process can also be used to validate and approve all new devices.
4. *Visibility/Attribution:* Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every

FTC-0002259

system that has an Internet Protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether or not they are attached to the organization's network.

5. *Configuration/Hygiene:* Make sure the asset inventory database is properly protected and a copy stored in a secure location.
6. *Configuration/Hygiene:* In addition to an inventory of hardware, organizations should develop an inventory of information assets that identifies their critical information and maps critical information to the hardware assets (including servers, workstations, and laptops) on which it is located. A department and individual responsible for each information asset should be identified, recorded, and tracked.
7. *Configuration/Hygiene:* Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. 802.1x must be tied into the inventory data to determine authorized vs. unauthorized systems.
8. *Configuration/Hygiene:* Deploy network access control (NAC) to monitor authorized systems so if attacks occur, the impact can be remediated by moving the untrusted system to a virtual local area network that has minimal access.
9. *Configuration/Hygiene:* Create separate VLANs for BYOD (bring your own device) systems or other untrusted devices.
10. *Advanced:* Utilize client certificates to validate and authenticate systems prior to connecting to the private network.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 2: Map the Network
Milestone 3: Network Architecture
Network Access Protection/Control (NAP/NAC)

Procedures and Tools to Implement and Automate this Control

Organizations must first establish information/asset owners, deciding and documenting which organizations and individuals are responsible for each component of a business process that includes information, software, and hardware. Some organizations maintain asset inventories using specific large-scale enterprise commercial products dedicated to the task, or they use free solutions to track and then sweep the network periodically for new assets connected to it. In particular, when organizations acquire new systems, they record the owner and features of each new asset, including its network interface media access control (MAC) address and location. This mapping of asset attributes and owner-to-MAC address can be stored in a free or commercial database management system.

Then, with the asset inventory assembled, many organizations use tools to pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network.

Going further, effective organizations configure free or commercial network scanning tools to perform network sweeps on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, organizations should verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks. In conducting inventory scans, scanning tools could send traditional ping packets (ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.

In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces looking for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems churn significantly. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused. Additionally, remote machines accessing the network using virtual private network (VPN) technology may appear on the network for a time, and then be disconnected from it. Whether physical or virtual, each machine using an IP address should be included in an organization's asset inventory.

Control 1 Metric

The system must be capable of identifying any new unauthorized devices that are connected to the network within 24 hours, and of alerting or sending e-mail notification to a list of enterprise administrative personnel. The system must automatically isolate the unauthorized system from the network within one hour of the initial alert and send a follow-up alert or e-mail notification when isolation is achieved. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until the unauthorized system has been removed from the network. The asset inventory database and alerting system must be able to identify the location, department, and other details of where authorized and unauthorized devices are plugged into the network. While the 24-hour and one-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even

FTC-0002261

more rapid alerting and isolation. With automated tools, notification about an unauthorized asset connected to the network can be sent within two minutes and isolation achieved within five minutes.

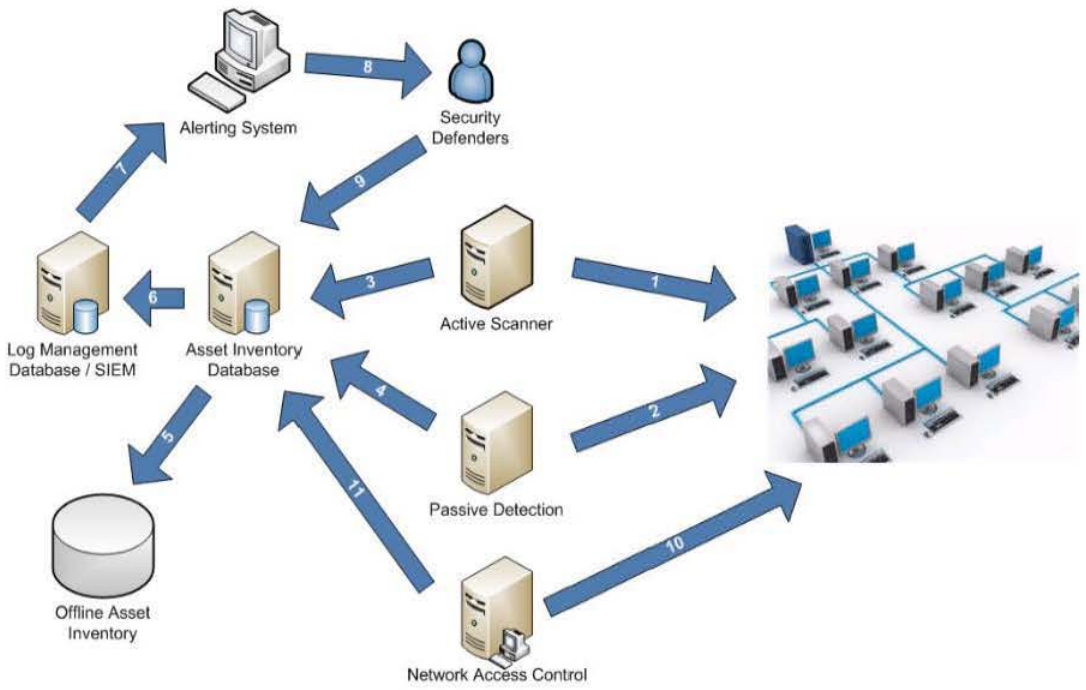
Control 1 Test

To evaluate the implementation of Control 1 on a periodic basis, the evaluation team will connect hardened test systems to at least 10 locations on the network, including a selection of subnets associated with demilitarized zones (DMZs), workstations, and servers. Two of the systems must be included in the asset inventory database, while the other systems are not. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the newly connected systems within 24 hours of the test machines being connected to the network. The evaluation team must verify that the system provides details of the location of all the test machines connected to the network. For those test machines included in the asset inventory, the team must also verify that the system provides information about the asset owner.

The evaluation team must then verify that the test systems are automatically isolated from the production network within one hour of initial notification and that an e-mail or alert indicating the isolation has occurred. The team must then verify that the connected test systems are isolated from production systems by attempting to ping and use other protocols to access systems on the production network and checking that connectivity is not allowed.

Control 1 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining hardware devices on the organization's network. These systems should be able to identify if new systems are introduced to the environment that have not been authorized by enterprise personnel. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify each of the process steps in order to help identify potential failure points in the overall control.

Step 1: Active device scanner scans network systems

Step 2: Passive device scanner captures system information

Step 3: Active scanner reports to inventory database

Step 4: Passive scanner reports to inventory database

Step 5: Inventory database stored offline

Step 6: Inventory database initiates alerting system

Step 7: Alert system notifies security defenders

Step 8: Security defenders monitor and secure inventory database

Step 9: Security defenders updates secure inventory database

Step 10: Network access control (NAC) continuously monitors network

Step 11: Network access control checks and provides updates to the asset inventory database

Critical Control 2: Inventory of Authorized and Unauthorized Software

The processes and tools organizations use to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.

How Do Attackers Exploit the Absence of this Control?

Computer attackers deploy systems that continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Without the ability to inventory and control which programs are installed and allowed to run on their machines, enterprises make their systems more vulnerable. Such poorly controlled machines are more likely to be either running software that is unneeded for business purposes, introducing potential security flaws, or running malware introduced by a computer attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Devise a list of authorized software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be tied to file integrity checking software to validate that the software has not be modified.
2. *Quick wins:* Perform regular scanning and generate alerts when unapproved software is installed on a computer. A strict change control process should also be implemented to control any changes or installation of software to any systems on the network.
3. *Visibility/Attribution:* Deploy application white listing technology that allows systems to run only approved software and prevents execution of all other software on the system.
4. *Visibility/Attribution:* Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number

and patch level. The software inventory should be tied to vulnerability reporting/threat intelligence services to fix vulnerable software proactively.

5. *Visibility/Attribution:* The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
6. *Configuration/Hygiene:* The software inventory tool should also monitor for unauthorized software installed on each machine. This unauthorized software also includes legitimate system administration software installed on inappropriate systems where there is no business need for it. Dangerous file types (e.g., exe, zip, msi, etc.) should be closely monitored and/or blocked.
7. *Configuration/Hygiene:* Software inventory and application white listing should also be deployed on all mobile devices that are utilized across the organization.
8. *Advanced:* Virtual machines and/or air-gapped systems should also be used to isolate and run applications that are required but based on higher risk and that should not be installed within a networked environment.
9. *Advanced:* Configure client workstations with nonpersistent virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.
10. *Advanced:* Deploy software that only provides signed software ID tags. A software identification tag is an XML file that is installed alongside software, and uniquely identifies the software, providing data for software inventory and asset management.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 7: Baseline Management
Executable Content Restrictions

Procedures and Tools to Implement and Automate this Control

Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Features that implement white and black lists of programs allowed to run or blocked from executing are included in many modern endpoint security suites. Moreover, commercial solutions are increasingly bundling together anti-virus, anti-spyware, personal firewall, and host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), along with application white and black listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these

tools offer custom white and black lists based on executable path, hash, or regular expression matching. Some even include a gray-list function that allows administrators to define rules for execution of specific programs only by certain users and at certain times of day, and black lists based on specific signatures.

Control 2 Metric

The system must be capable of identifying unauthorized software by detecting either an attempt to install it or execute it, notifying enterprise administrative personnel within 24 hours through an alert or e-mail. Systems must block installation, prevent execution, or quarantine unauthorized software within one additional hour, alerting or sending e-mail when this action has occurred. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until the unauthorized system has been removed from the network. While the 24-hour and one-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting and isolation.

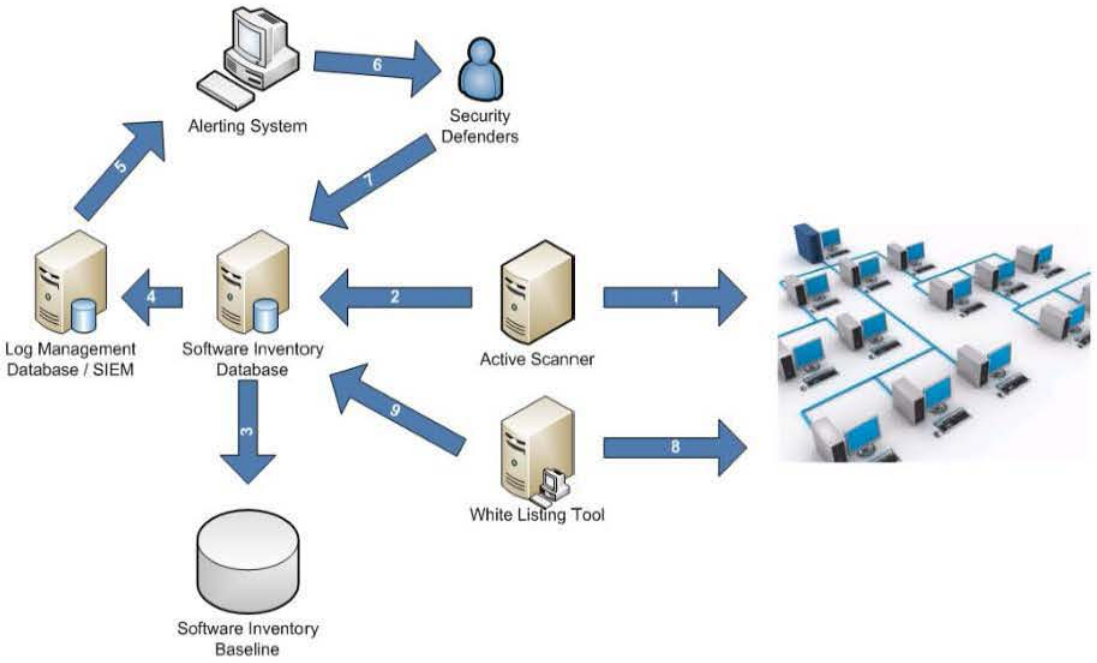
Control 2 Test

To evaluate the implementation of Control 2 on a periodic basis, the evaluation team must move a benign software test program that is not included in the authorized software list to 10 systems on the network. Two of the systems must be included in the asset inventory database, while the other systems do not need to be included. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the new software within 24 hours. The team must also verify that the alert or e-mail is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team must verify that the system provides details of the location of each machine with this new test software, including information about the asset owner.

The evaluation team must then verify that the software is blocked by attempting to execute it and verifying that the software is not allowed to run.

Control 2 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining software installed on the organization's network systems. These systems should be able to identify if new software is introduced to the environment that has not been authorized by enterprise personnel. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Active device scanner

Step 2: Active scanner reports to inventory database

Step 3: Inventory database compares to inventory baseline

Step 4: Inventory database initiates alerting system

Step 5: Alert system notifies security defenders

Step 6: Security defenders monitor and secure inventory database.

Step 7: Security defenders updates software inventory database

Step 8: White listing tool continuously monitors all systems on the network

Step 9: White listing checks and makes updates to the software inventory database

Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.

How Do Attackers Exploit the Absence of this Control?

On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way it was delivered from manufacturers and resellers, thereby being immediately vulnerable to exploitation. Default configurations are often geared to ease-of-deployment and ease-of-use and not security, leaving extraneous services that are exploitable in their default state. In addition, patches are not always applied in a timely manner and software updates often introduce unknown weaknesses into a piece of software that can be exploited by zero-day exploits. Attackers attempt to exploit both network-accessible services and browsing client software using such techniques.

Defenses against these automated exploits include procuring computer and network components with the secure configurations already implemented, deploying such pre-configured hardened systems, updating these configurations on a regular basis, and tracking them in a configuration management system.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Strict configuration management should be followed, building a secure image that is used to build all new systems that are deployed to the enterprise. Any existing system that becomes compromised is re-imaged with the secure build. Regular updates to this image are integrated into the organization's change management processes. Images should be created for both workstations and servers.
2. *Quick wins:* System images must have documented security settings that are tested before deployment, approved by an organization change control board, and registered with a central image library for the organization or multiple organizations. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
3. *Quick wins:* Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system, such as those released by the NIST, NSA, Defense Information Systems Agency (DISA), Center for Internet Security (CIS), and others. This hardening would typically include removal of unnecessary accounts, disabling or removal of unnecessary services, and configuring nonexecutable stacks and heaps. Such hardening also involves, among other measures, applying patches, closing open and unused network ports, implementing intrusion detection systems and/or intrusion prevention systems, and erecting host-based firewalls.
4. *Quick wins:* The master images themselves must be stored on securely configured servers, with integrity checking tools and change management to ensure that only

authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network. Images should be tested at the hot or warm disaster recovery site if one is available.

5. *Quick wins:* Run the last version of software and make sure it is fully patched. Remove outdated or older software from the system.
6. *Visibility/Attribution:* Any deviations from the standard build or updates to the standard build should be approved by a change control board and documented in a change management system.
7. *Visibility/Attribution:* Negotiate contracts to buy systems configured securely out of the box using standardized images, which should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities.
8. *Visibility/Attribution:* Utilize application white listing to control and manage any configuration changes to the software running on the system.
9. *Configuration/Hygiene:* All remote administration of servers, workstation, network devices, and similar equipment shall be done over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.
10. *Configuration/Hygiene:* Utilize file integrity checking tools on at least a weekly basis to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. All alterations to such files should be automatically reported to security personnel. The reporting system should have the ability to account for routine and expected changes, highlighting unusual or unexpected alterations.
11. *Configuration/Hygiene:* Implement and test an automated configuration monitoring system that measures all secure configuration elements that can be measured through remote testing, using features such as those included with tools compliant with Security Content Automation Protocol (SCAP) to gather configuration vulnerability information. These automated tests should analyze both hardware and software changes, network configuration changes, and any other modifications affecting security of the system.
12. *Configuration/Hygiene:* Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for Unix systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
13. *Advanced:* Organizations need to adopt a formal process and management infrastructure for configuration control of mobile devices. The process needs to include secure remote wiping of lost or stolen devices, approval of corporate apps, and denial of unapproved apps. If the device is owned by the organization, a full wipe should be performed. If it is a BYOD system, a selective wipe should be performed, removing the organization's information.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 7: Baseline Management
Configuration and Change Management

Procedures and Tools to Implement and Automate this Control

Organizations can implement this control by developing a series of images and secure storage servers for hosting these standard images. Commercial and/or free configuration management tools can then be employed to measure the settings operating system and applications of managed machines to look for deviations from the standard image configurations used by the organization. Some configuration management tools require that an agent be installed on each managed system, while others remotely log in to each managed machine using administrator credentials. Either approach or a combination of the two approaches can provide the information needed for this control.

Control 3 Metric

The system must be capable of identifying any changes to an official hardened image that may include modifications to key files, services, ports, configuration files, or any software installed on the system. Modifications include deletion, changes, or additions of new software to any part of the operating systems, services, or applications running on the system. The configuration of each system must be checked against the official master image database to verify any changes to secure configurations that would impact security. Any of these changes to a computer system must be detected within 24 hours and notification performed by alerting or sending e-mail notification to a list of enterprise administrative personnel. Systems must block installation, prevent execution, or quarantine unauthorized software within one additional hour, alerting or sending e-mail when this action has occurred. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until the unauthorized system has been removed from the network or remediated. While the 24-hour and one-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting and isolation.

Control 3 Test

To evaluate the implementation of Control 3 on a periodic basis, an evaluation team must move a benign test system that does not contain the official hardened image, but that does contain additional services, ports, and configuration files changes onto the network. This must be performed on 10 different random segments using either real or virtual systems. The evaluation team must then verify that the systems generate an alert regarding the changes to the software within 24 hours. It is important that the evaluation team verify that all unauthorized changes have

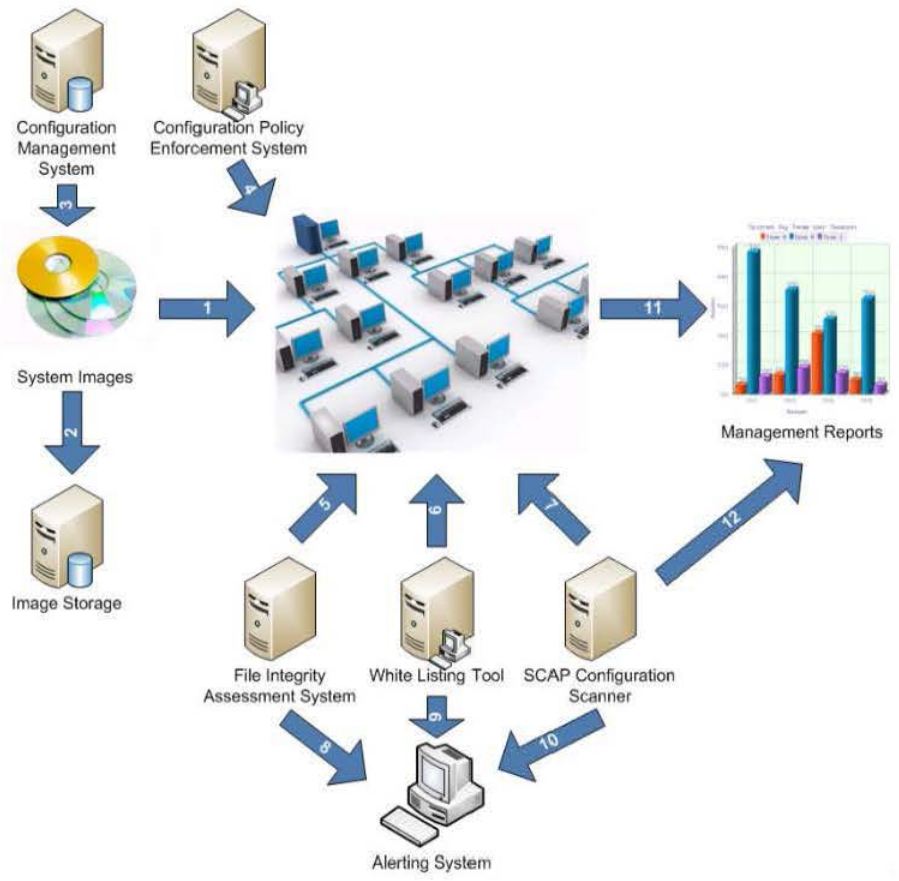
been detected. The team must also verify that the alert or e-mail is received within one additional hour indicating that the software has been blocked or quarantined. The evaluation team must verify that the system provides details of the location of each machine with the unauthorized changes, including information about the asset owner.

The evaluation team must then verify that the software is blocked by attempting to execute it and verifying that it is not allowed to run. In addition to these tests, two additional tests must be performed:

1. File integrity checking tools must be run on a regular basis. Any changes to critical operating system, services, and configuration files must be checked on an hourly basis. Any changes must be blocked and follow the above notification process.
2. System scanning tools that check for software version, patch levels, and configuration files must be run on a daily basis. Any changes must be blocked and follow the above e-mail notification process.

Control 3 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement the, test the controls, and identify where potential failures in the system might occur. As with any configurations, all changes must be approved and managed by a change control process.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the devices, software, and entities used to manage and implement consistent configuration settings to workstations, laptops, and servers on the network. We will be discussing other network devices later in the course. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify each step in order to identify potential failure points in the overall control.

Step 1: Secured system images applied to computer systems

Step 2: Secured system images stored in a secure manner

Step 3: Configuration management system validates and checks system images

Step 4: Configuration policy enforcement system actively scans production systems for misconfigurations or deviations from baselines

Step 5: File integrity assessment systems monitor critical system binaries and data sets

Step 6: White listing tool monitors systems configurations and software

Step 7: SCAP configuration scanner validates configurations

Step 8: File integrity assessment system sends deviations to alerting system

Step 9: White listing tool sends deviations to alerting system

Step 10: SCAP configuration scanner sends deviations to alerting system

Step 11 and 12: Management reports document configuration status

Critical Control 4: Continuous Vulnerability Assessment and Remediation

The processes and tools used to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database.

How Do Attackers Exploit the Absence of this Control?

Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Organizations that do not scan for vulnerabilities and address discovered flaws proactively face a significant likelihood of having their computer systems compromised. Vulnerabilities must also be tied to threat intelligence and be properly prioritized.

As vulnerability scans become more common, attackers are utilizing them as a point of exploitation. It is important to carefully control authenticated vulnerability scans and the associated administrator account. Attackers will take over one machine with local privileges, and wait for an authenticated scan to occur against the machine. When the scanner logs in with domain admin privileges, the attacker either grabs the token of the logged-in scanning tool, or sniffs the challenge response and cracks it. Either way, the attacker then can pivot anywhere else in the organization as domain admin.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Run automated vulnerability scanning tools against all systems on their networks on a weekly or more frequent basis using a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (CVE) and configuration-based vulnerabilities (CCE). Where feasible, vulnerability scanning should occur on a daily basis using an up-to-date vulnerability scanning tool. Any vulnerability identified should be remediated in a timely manner, with critical vulnerabilities fixed within 48 hours.
2. *Quick wins:* Event logs should be correlated with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools themselves is logged. Second, personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.
3. *Quick wins:* Utilize a dedicated account for authenticated vulnerability scans. The scanning account should not be used for any other administrative activities and tied to specific IP addresses. Ensure only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.
4. *Quick wins:* Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures.
5. *Visibility/Attribution:* Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools

are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

6. *Visibility/Attribution:* Carefully monitor logs associated with any scanning activity and associated administrator accounts to ensure that all scanning activity and associated access via the privileged account is limited to the timeframes of legitimate scans.
7. *Configuration/Hygiene:* In addition to unauthenticated vulnerability scanning, organizations should ensure that all vulnerability scanning is performed in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.
8. *Configuration/Hygiene:* Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.
9. *Configuration/Hygiene:* Vulnerability scanning tools should be tuned to compare services that are listening on each machine against a list of authorized services. The tools should be further tuned to identify changes over time on systems for both authorized and unauthorized services.
10. *Configuration/Hygiene:* Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the organization. Alternative countermeasures should be considered if patches are not available.
11. *Configuration/Hygiene:* Critical patches must be evaluated in a test environment before being pushed into production on enterprise systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality.
12. *Configuration/Hygiene:* Address the most damaging vulnerabilities first. Prioritize the vulnerable assets based on both the technical and organization-specific business risks. An industry-wide or corporate-wide vulnerability ranking may be inadequate to prioritize which specific assets to address first. A phased rollout can be used to minimize the impact to the organization.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 6: Patch Management

Procedures and Tools to Implement and Automate this Control

A large number of vulnerability scanning tools are available to evaluate the security configuration of systems. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities in multiple departments of an organization or even across organizations, it is preferable to use vulnerability scanning tools that measure security flaws and map them to vulnerabilities and issues categorized using one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: CVE, CCE, OVAL, CPE, CVSS, and/or XCCDF.

Advanced vulnerability scanning tools can be configured with user credentials to log in to scanned systems and perform more comprehensive scans than can be achieved without login credentials. The frequency of scanning activities, however, should increase as the diversity of an organization's systems increases to account for the varying patch cycles of each vendor.

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of local machines on which they are installed. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses by administrators.

Effective organizations link their vulnerability scanners with problem-ticketing systems that automatically monitor and report progress on fixing problems, and that make unmitigated critical vulnerabilities visible to higher levels of management to ensure the problems are solved.

The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

As vulnerabilities related to unpatched systems are discovered by scanning tools, security personnel should determine and document the amount of time that elapses between the public release of a patch for the system and the occurrence of the vulnerability scan. If this time window exceeds the organization's benchmarks for deployment of the given patch's criticality level, security personnel should note the delay and determine if a deviation was formally documented for the system and its patch. If not, the security team should work with management to improve the patching process.

Additionally, some automated patching tools may not detect or install certain patches due to error by the vendor or administrator. Because of this, all patch checks should reconcile system patches with a list of patches each vendor has announced on its website.

Control 4 Metric

All machines identified by the asset inventory system associated with Critical Control 1 must be scanned for vulnerabilities. Additionally, if the vulnerability scanner identifies any devices not included in the asset inventory, it must alert or send e-mail to enterprise administrative personnel within 24 hours. The system must be able to alert or e-mail enterprise administrative personnel

within one hour of weekly or daily automated vulnerability scans being completed. If a scan cannot be completed successfully, the system must alert or send e-mail to administrative personnel within one hour indicating that the scan has not completed successfully. Every 24 hours after that point, the system must alert or send e-mail about the status of uncompleted scans, until normal scanning resumes.

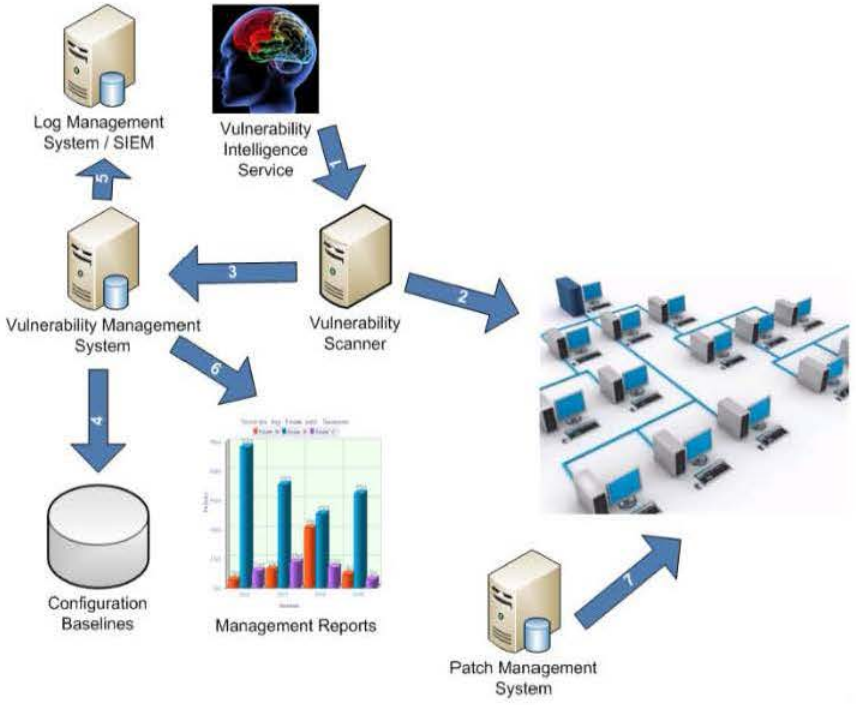
Automated patch management tools must alert or send e-mail to administrative personnel within 24 hours of the successful installation of new patches. While the 24-hour and one-hour timeframes represent the current metric to help organizations improve their state of security, in the future, organizations should strive for even more rapid alerting, with notification about an unauthorized asset connected to the network or an incomplete vulnerability scan sent within two minutes.

Control 4 Test

To evaluate the implementation of Control 4 on a periodic basis, the evaluation team must verify that scanning tools have successfully completed their weekly or daily scans for the previous 30 cycles of scanning by reviewing archived alerts and reports to ensure that the scan was completed. If a scan could not be completed in that timeframe, the evaluation team must verify that an alert or e-mail was generated indicating that the scan did not finish.

Control 4 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement tem, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, the vulnerability scanners, management system, patch management systems, and configuration baselines all work together to address an organization's vulnerability management and remediation strategy. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Vulnerability intelligence service provides inputs to vulnerability scanner

Step 2: Vulnerability scanners scan production systems

Step 3: Vulnerability scanners report detected vulnerabilities to a vulnerability management system (VMS)

Step 4: The VMS compares production systems to configuration baselines

Step 5: The VMS sends information to log management correlation system

Step 6: The VMS produces reports for management

Step 7: A patch management system applies software updates to production systems

FTC-0002279

Critical Control 5: Malware Defenses

The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.

How Do Attackers Exploit the Absence of this Control?

Malicious software is an integral and dangerous aspect of Internet threats, targeting end-users and organizations via web browsing, e-mail attachments, mobile devices, the cloud, and other vectors. Malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems. Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system. Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block its execution.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. The endpoint security solution should include zero-day protection such as network behavioral heuristics.
2. *Quick wins:* Employ anti-malware software and signature auto-update features or have administrators manually push updates to all machines on a daily basis. After applying an update, automated systems should verify that each system has received its signature update.
3. *Quick wins:* Configure laptops, workstations, and servers so that they will not auto-run content from USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, Firewire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media. If the devices are not required for business use, they should be disabled.
4. *Quick wins:* Configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.
5. *Quick wins:* All e-mail attachments entering the organization's e-mail gateway should be scanned and blocked if they contain malicious code or file types unneeded for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.
6. *Quick wins:* Apply anti-virus scanning at the Web Proxy gateway. Content filtering for file-types should be applied at the perimeter.
7. *Quick wins:* Deploy features and toolkits such as Data Execution Prevention (DEP) and Enhanced Mitigation Experience Toolkit (EMET), products that provide sandboxing (e.g., run browsers in a VM), and other techniques that prevent malware exploitation.
8. *Quick wins:* Limit use of external devices to those that have business need. Monitor for use and attempted use of external devices.

9. *Visibility/Attribution:* Block access to external e-mail systems, instant messaging services and other social media tools.
10. *Visibility/Attribution:* Automated monitoring tools should use behavior-based anomaly detection to complement and enhance traditional signature-based detection.
11. *Visibility/Attribution:* Utilize network-based anti-malware tools to analyze all inbound traffic and filter out malicious content before it arrives at the endpoint.
12. *Advanced:* Continuous monitoring should be performed on all inbound and outbound traffic. Any large transfers of data or unauthorized traffic should be flagged and, if validated as malicious, the computer should be moved to an isolated VLAN.
13. *Advanced:* Implement an incident response process that allows their IT Support Organization to supply their Security Team with samples of malware running undetected on corporate systems. Samples should be provided to the security vendor for "out-of-band" signature creation and deployed to the enterprise by system administrators.
14. *Advanced:* Utilize network-based flow analysis tools to analyze inbound and outbound traffic looking for anomalies, indicators of malware, and compromised systems.
15. *Advanced:* Deploy "reputation-based technologies" on all endpoint devices to cover the gap of signature based technologies.
16. Advanced: Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.
17. *Advanced:* Apply proxy technology to all communication between internal network and the Internet.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Virus Scanners and Host Intrusion Prevention Systems (HIPS)
Personal Electronic Device (PED) Management
Network Access Protection/Control (NAP/NAC)
Security Gateways, Proxies, and Firewalls
Network Security Monitoring

Procedures and Tools to Implement and Automate this Control

Relying on policy and user action to keep anti-malware tools up to date has been widely discredited, as many users have not proven capable of consistently handling this task. To ensure anti-virus signatures are up to date, organizations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, anti-spyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Some enterprises deploy free or commercial honeypot and tarpit tools to identify attackers in their environment. Security personnel should continuously monitor honeypots and tarpits to

determine whether traffic is directed to them and account logins are attempted. When they identify such events, these personnel should gather the source address from which this traffic originates and other details associated with the attack for follow-on investigation.

Control 5 Metric

The system must identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system within one hour, alerting or sending e-mail notification to a list of enterprise personnel via their centralized anti-malware console or event log system. Systems must block installation, prevent execution, or quarantine malicious software within one hour, alerting or sending e-mail when this action has occurred. Every 24 hours after that point, the system must alert or send e-mail about the status of the malicious code until such time as the threat has been completely mitigated on that system. While the one-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid detection and malware isolation.

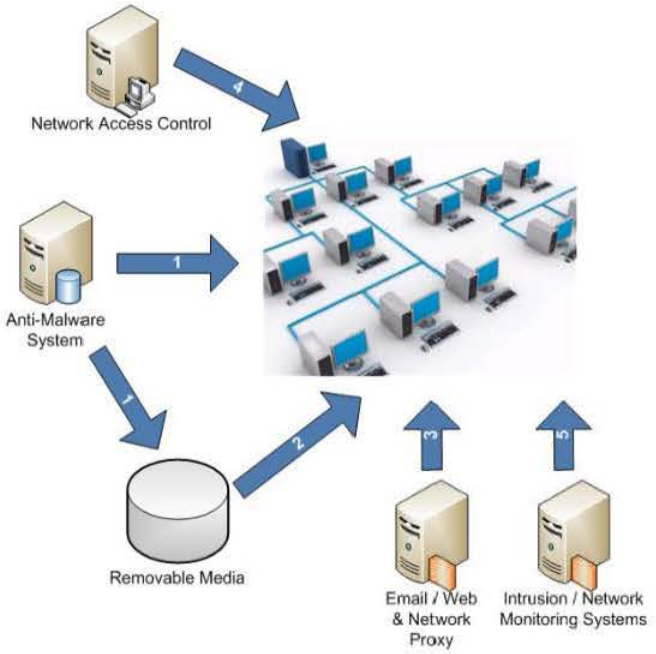
Control 5 Test

To evaluate the implementation of Control 5 on a periodic basis, the evaluation team must move a benign software test program that appears to be malware (such as an EICAR file or benign hacker tools) but that is not included in the official authorized software list to 10 systems on the network via a network share. The selection of these systems must be as random as possible and include a cross-section of the organization's systems and locations. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the benign malware within one hour. The team must also verify that the alert or e-mail indicating that the software has been blocked or quarantined is received within one hour. The evaluation team must verify that the system provides details of the location of each machine with this new test file, including information about the asset owner. The team must then verify that the file is blocked by attempting to execute or open it and verifying that it is not allowed to be accessed.

Once this test has been performed transferring the files to organization systems via removable media, the same test must be repeated, but this time transferring the benign malware to 10 systems via e-mail instead. The organization must expect the same notification results as noted with the removable media test.

Control 5 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining anti-malware systems and threat vectors such as removable media. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Anti-malware systems analyzes production systems and removable media

Step 2: Removable media is analyzed when connected to production systems

Step 3: Email/web and network proxy devices analyze all incoming and outgoing traffic

Step 4: Network access control monitors all systems connected to the network

Step 5: Intrusion / network monitoring systems performs continuous monitoring looking for signs of malware

Critical Control 6: Application Software Security

The processes and tools organizations use to detect/prevent/correct security weaknesses in the development and acquisition of software applications.

How Do Attackers Exploit the Absence of this Control?

Attacks against vulnerabilities in web-based and other application software have been a top priority for criminal organizations in recent years. Application software that does not properly check the size of user input, fails to sanitize user input by filtering out unneeded but potentially malicious character sequences, or does not initialize and clear variables properly could be vulnerable to remote compromise. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. In one attack, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

To avoid such attacks, both internally developed and third-party application software must be carefully tested to find security flaws. For third-party application software, enterprises should verify that vendors have conducted detailed security testing of their products. For in-house developed applications, enterprises must conduct such testing themselves or engage an outside firm to conduct it.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
2. *Visibility/Attribution:* At a minimum, explicit error checking should be done for all input. Whenever a variable is created in source code, the size and type should be determined. When input is provided by the user it should be verified that it does not exceed the size or the data type of the memory location in which it is stored or moved in the future.
3. *Visibility/Attribution:* Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application and on a regular recurring basis. Organizations should understand how their applications behave under denial of service or resource exhaustion attacks.

4. *Visibility/Attribution:* System error messages should not be displayed to end-users (output sanitization).
5. *Visibility/Attribution:* Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.
6. *Configuration/Hygiene:* Test in-house-developed and third-party-procured web and other application software for coding errors and malware insertion, including backdoors, prior to deployment using automated static code analysis software. If source code is not available, these organizations should test compiled code using static binary analysis tools. In particular, input validation and output encoding routines of application software should be carefully reviewed and tested.
7. *Configuration/Hygiene:* For applications that rely on a database, organizations should conduct a configuration review of both the operating system housing the database and the database software itself, checking settings to ensure that the database system has been hardened using standard hardening templates. All systems that are part of critical business processes should also be tested.
8. *Configuration/Hygiene:* Ensure that all software development personnel receive training in writing secure code for their specific development environment.
9. *Configuration/Hygiene:* Sample scripts, libraries, components, compilers, or any other unnecessary code that is not being used by an application should be uninstalled or removed from the system.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 3: Network Architecture
Milestone 7: Baseline Management
Security Gateways, Proxies, and Firewalls

Procedures and Tools to Implement and Automate this Control

Source code testing tools, web application security scanning tools, and object code testing tools have proven useful in securing application software, along with manual application security penetration testing by testers who have extensive programming knowledge and application penetration testing expertise. The Common Weakness Enumeration (CWE) initiative is used by many such tools to identify the weaknesses that they find. Organizations can also use CWE to determine which types of weaknesses they are most interested in addressing and removing. When evaluating the effectiveness of testing for these weaknesses, MITRE's Common Attack Pattern Enumeration and Classification can be used to organize and record the breadth of the testing for the CWEs and to enable testers to think like attackers in their development of test cases.

Control 6 Metric

The system must be capable of detecting and blocking an application-level software attack, and must generate an alert or send e-mail to enterprise administrative personnel within 24 hours of detection and blocking.

All Internet-accessible web applications must be scanned on a weekly or daily basis, alerting or sending e-mail to administrative personnel within 24 hours of completing a scan. If a scan cannot be completed successfully, the system must alert or send e-mail to administrative personnel within one hour indicating that the scan has been unsuccessful. Every 24 hours after that point, the system must alert or send e-mail about the status of uncompleted scans, until normal scanning resumes.

Additionally, all high-risk vulnerabilities in Internet-accessible web applications identified by web application vulnerability scanners, static analysis tools, and automated database configuration review tools must be mitigated (by either fixing the flaw or implementing a compensating control) within 15 days of discovery of the flaw.

While the 24-hour and one-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting, with notification about an application attack attempt sent within two minutes.

Control 6 Test

To evaluate the implementation of Control 6 on a monthly basis, an evaluation team must use a web application vulnerability scanner to test for each type of flaw identified in the regularly updated list of the "25 Most Dangerous Programming Errors" by MITRE and the SANS Institute. The scanner must be configured to assess all of the organization's Internet-accessible web applications to identify such errors. The evaluation team must verify that the scan is detected within 24 hours and that an alert is generated.

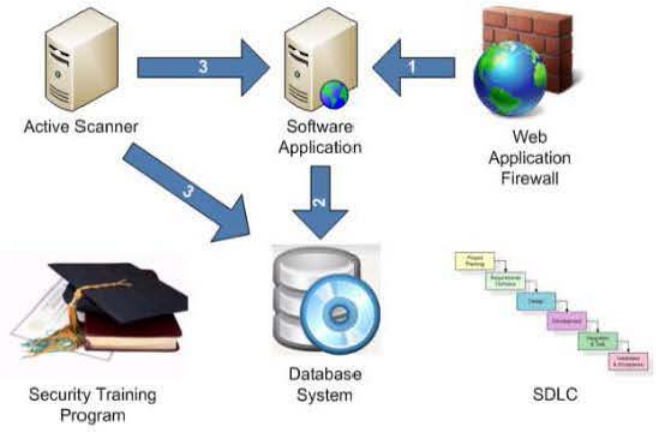
In addition to the web application vulnerability scanner, the evaluation team must also run static code analysis tools and database configuration review tools against Internet-accessible applications to identify security flaws on a monthly basis.

The evaluation team must verify that all high-risk vulnerabilities identified by the automated vulnerability scanning tools or static code analysis tools have been remediated or addressed through a compensating control (such as a web application firewall) within 15 days of discovery.

The evaluation team must verify that application vulnerability scanning tools have successfully completed their regular scans for the previous 30 cycles of scanning by reviewing archived alerts and reports to ensure that the scan was completed. If a scan was not completed successfully, the system must alert or send e-mail to enterprise administrative personnel indicating what happened. If a scan could not be completed in that timeframe, the evaluation team must verify that an alert or e-mail was generated indicating that the scan did not finish.

Control 6 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the process of monitoring applications and using tools that enforce a security style when developing applications.

The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Web application firewalls protect connections to internal web applications

Step 2: Software applications securely connect to database systems

Step 3: Code analysis and vulnerability scanning tools scan application systems and database systems

FTC-0002287

Critical Control 7: Wireless Device Control

The processes and tools used to track/control/prevent/correct the security use of wireless LANS (local area networks), access points, and wireless client systems.

How Do Attackers Exploit the Absence of this Control?

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
2. *Quick wins:* Ensure that all wireless access points are manageable using enterprise management tools. Access points designed for home use often lack such enterprise management capabilities, and should therefore be avoided in enterprise environments.
3. *Quick wins:* Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.
4. *Visibility/Attribution:* Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.
5. *Visibility/Attribution:* 802.1x should be used to control which devices are allowed to connect to the wireless network.
6. *Visibility/Attribution:* A site survey should be performed to determine what areas within the organization need coverage. After the wireless access points are strategically placed, the signal strength should be tuned to minimize leakage to areas that do not need coverage.
7. *Configuration/Hygiene:* Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks.
8. *Configuration/Hygiene:* For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system

or extensible firmware interface), with password protections to lower the possibility that the user will override such configurations.

9. *Configuration/Hygiene:* Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least WiFi Protected Access 2 (WPA2) protection.
10. *Configuration/Hygiene:* Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.
11. *Configuration/Hygiene:* Ensure that wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.
12. *Configuration/Hygiene:* Disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.
13. *Configuration/Hygiene:* Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.
14. *Configuration/Hygiene:* Wireless access points should never be directly connected to the private network. They should either be placed behind a firewall or put on a separate VLAN so all traffic can be examined and filtered.
15. *Configuration/Hygiene:* All mobile devices, including personnel devices, must be registered prior to connecting to the wireless network. All registered devices must be scanned and follow the corporate policy for host hardening and configuration management.
16. *Advanced:* Configure all wireless clients used to access private networks or handle organization data in a manner so that they cannot be used to connect to public wireless networks or any other networks beyond those specifically allowed by the organization.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Remote Access Security

Procedures and Tools to Implement and Automate this Control

Effective organizations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.

Additionally, the security team should periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates. When devices relying on weak wireless security settings are identified, they should be found within the organization's asset inventory and either reconfigured more securely or denied access to the organization network.

Additionally, the security team should employ remote management tools on the wired network to pull information about the wireless capabilities and devices connected to managed systems.

Control 7 Metric

The system must be capable of identifying unauthorized wireless devices or configurations when they are within range of the organization's systems or connected to their networks. The system must be capable of identifying any new unauthorized wireless devices that associate or join the network within one hour, alerting or sending e-mail notification to a list of enterprise personnel. The system must automatically isolate an attached wireless access point from the network within one hour and alert or send e-mail notification when isolation is achieved. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until it has been removed from the network. The asset inventory database and alerting system must be able to identify the location, department, and other details of where authorized and unauthorized wireless devices are plugged into the network. While the 24-hour and one-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting and isolation, with notification about an unauthorized wireless devices sent within two minutes and isolation within five minutes.

Control 7 Test

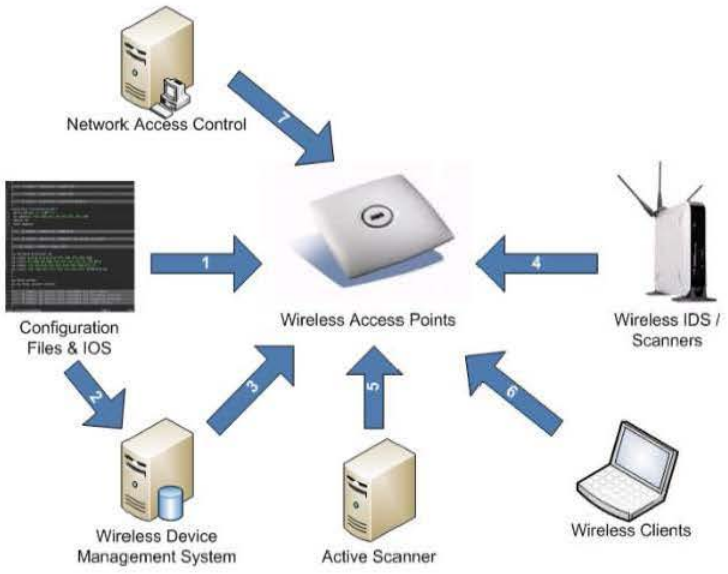
To evaluate the implementation of Control 7 on a periodic basis, the evaluation team staff must configure 10 unauthorized but hardened wireless clients and wireless access points to the organization's network and attempt to connect them to its wireless networks. In the case of wireless access points, these access points must not be directly connected to the organization's trusted network. Instead, they must simply be configured to act as a wireless gateway without physically connecting to a wired network interface. In the case of scanning for wireless access points from a wired interface, the connected access point must have the wireless radio disabled for the duration of the test. These systems must be configured to test each of the following scenarios:

- A wireless client with an unauthorized service set identifier configured on it.
- A wireless client with improper encryption configured.
- A wireless client with improper authentication configured.
- A wireless access point with improper encryption configured.
- A wireless access point with improper authentication configured.
- A completely rogue wireless access point using an unauthorized configuration.

When any of the above-noted systems attempt to connect to the wireless network, an alert must be generated and enterprise staff must respond to the alerts to isolate the detected device or remove the device from the network.

Control 7 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the configuration and management of wireless devices, wireless IDS/scanners, wireless device management systems, and vulnerability scanners. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Hardened configurations applied to wireless devices

Step 2: Hardened configurations managed by a configuration management system

Step 3: Configuration management system manages the configurations on wireless devices

Step 4: Wireless IDS monitor usage of wireless communications

Step 5: Vulnerability scanners scan wireless devices for potential vulnerabilities

Step 6: Wireless clients utilize wireless infrastructure systems in a secure manner

Critical Control 8: Data Recovery Capability

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Note: This control has one or more sub-controls that must be validated manually.

How Do Attackers Exploit the Absence of this Control?

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. All backup policies should be compliant with any regulatory or official requirements.
2. *Quick wins:* Data on backup media should be tested on a regular basis by performing a data restoration process to ensure that the backup is properly working.
3. *Quick wins:* Key personal should be trained on both the backup and restoration processes. To be ready in case a major incident occurs, alternative personnel should also be trained on the restoration process just in case the primary IT point of contact is not available.
4. *Configuration/Hygiene:* Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
5. *Configuration/Hygiene:* Backup media, such as hard drives and tapes, should be stored in physically secure, locked facilities. End-of-life backup media should be securely erased/destroyed.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CP-9 (a, b, d, 1, 3), CP-10 (6)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

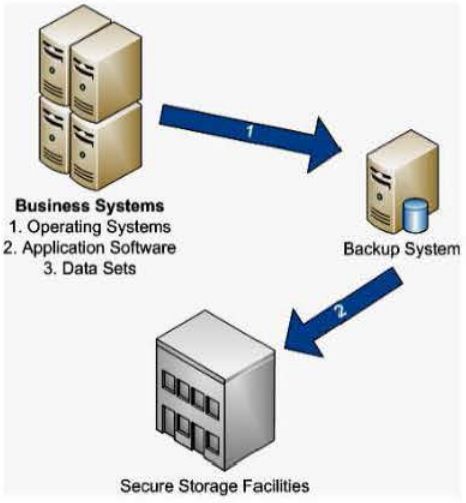
Backup Strategy

Procedures and Tools to Implement and Automate this Control

Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

Control 8 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining an organization's capability to restore systems in the event that data needs to be restored because of a data loss or breach of a system. While backups are certainly an important part of this process, the ability to restore data is the critical component. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Production business systems backed up on a regular basis to authorized organizational backup systems

Step 2: Backups created are stored offline at secure storage facilities.

Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps

The process and tools to make sure an organization understands the technical skill gaps within its workforce, including an integrated plan to fill the gaps through policy, training, and awareness.

Note: This control has one or more sub-controls that must be validated manually.

How Do Attackers Exploit the Absence of this Control?

The following are the skills of five groups of people constantly being tested by attackers:

1. End-users are fooled via social engineering scams in which they are tricked into providing passwords, opening attachments, loading software from untrusted sites, or visiting malicious web sites.
2. System administrators are also fooled in the same manner as normal users but are also tested when attackers attempt to trick the administrator into setting up unauthorized accounts.
3. Security operators and analysts are tested with new and innovative attacks introduced on a continual basis.
4. Application programmers are tested by criminals who find and exploit the vulnerabilities in the code that they write.
5. To a lesser degree, system owners are tested when they are asked to invest in cyber security but are unaware of the devastating impact a compromise and data exfiltration or alteration would have on their mission.

Any organization that hopes to be ready to find and respond to attacks effectively must find the gaps in its knowledge and provide exercises and training to fill those gaps. A solid security skills assessment program can provide actionable information to decision-makers about where security awareness needs to be improved, and can also help determine proper allocation of limited resources to improve security practices.

Training is also closely tied to policy and awareness. Policies tell people what to do, training provides them the skills to do it, and awareness changes behaviors so that people follow the policy. Training should be mapped against the skills required to perform a given job. If after training, users are still not following the policy, that policy should be augmented with awareness.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Perform gap analysis to see which security areas employees are not adhering to and use this as the basis for an awareness program. Organizations should devise periodic security awareness assessments to be given to employees and contractors on at least an annual basis in order to determine whether they understand the information security policies and procedures, as well as their role in those procedures.

2. *Quick wins:* Develop security awareness training for various personnel job descriptions. The training should include specific, incident-based scenarios showing the threats an organization faces, and should present proven defenses against the latest attack techniques.
3. *Quick wins:* Awareness should be carefully validated with policies and training. Policies tell users what to do, training provides them the skills to do it, and awareness changes their behavior so that they understand the importance of following the policy.
4. *Visibility/Attribution:* Metrics should be created for all policies and measured on a regular basis. Awareness should focus on the areas that are receiving the lowest compliance score.
5. *Configuration/Hygiene:* Conduct periodic exercises to verify that employees and contractors are fulfilling their information security duties by conducting tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller.
6. *Configuration/Hygiene:* Provide awareness sessions for users who are not following policies after they have received appropriate training.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AT-1, AT-2 (1), AT-3 (1)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

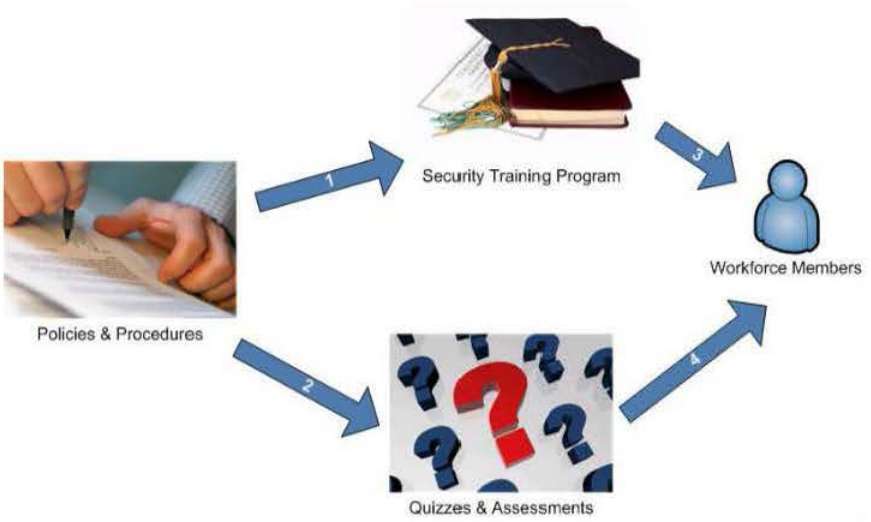
Training

Procedures and Tools to Implement and Automate this Control

The key to upgrading skills is measurement through assessments that show both the employee and the employer where knowledge is sufficient and where the gaps are. Once the gaps have been identified, those employees who have the requisite skills and knowledge can be called upon to mentor the employees who need to improve their skills. In addition, the organization can develop training programs that directly fill the gaps and maintain employee readiness.

Control 9 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the importance of educating workforce members in the security knowledge that they need in order to best perform their roles and responsibilities within the organization. The following list of the steps in the above diagram show how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Create training and awareness programs about the organization's information security policies and procedures

Step 2: Design quizzes and assessments about the organization's information security policies and procedures

Step 3: Present the training and awareness program to the organization's workforce

Step 4: Present the quizzes and assessments to the organization's workforce and validate the understanding of the information presented in the training and awareness program

Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

The processes and tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.

How Do Attackers Exploit the Absence of this Control?

Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, as the exceptions are deployed, and as those exceptions are not undone when the business need is no longer applicable. Making matters worse, in some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to gain access to target networks, redirect traffic on a network (to a malicious system masquerading as a trusted system), and intercept and alter information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.
2. *Quick wins:* At network interconnection points—such as Internet gateways, inter-organization connections, and internal network segments with different security controls—implement ingress and egress filtering to allow only those ports and protocols with an explicit and documented business need. All other ports and protocols should be blocked with default-deny rules by firewalls, network-based IPS, and/or routers.
3. *Configuration/Hygiene:* All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
4. *Configuration/Hygiene:* Network filtering technologies employed between networks with different security levels (firewalls, network-based IPS tools, and routers with access controls lists) should be deployed with capabilities to filter Internet Protocol version 6 (IPv6) traffic. However, if IPv6 is not currently being used it should be disabled. Since

many operating systems today ship with IPv6 support activated, filtering technologies need to take it into account.

5. *Configuration/Hygiene:* Network devices should be managed using two-factor authentication and encrypted sessions.
6. *Configuration/Hygiene:* The latest stable version of any security-related updates must be installed within 30 days of the update being released from the device vendor.
7. *Advanced:* The network infrastructure should be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), IA-2 (1, 6), IA-5, IA-8, RA-5, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18), SC-9

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 7: Baseline Management
Configuration and Change Management

Procedures and Tools to Implement and Automate this Control

Some organizations use commercial tools that evaluate the rule set of network filtering devices to determine whether they are consistent or in conflict, providing an automated sanity check of network filters and search for errors in rule sets or access controls lists (ACLs) that may allow unintended services through the device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

Control 10 Metric

The system must be capable of identifying any changes to network devices, including routers, switches, firewalls, and IDS and IPS systems. These changes include any modifications to key files, services, ports, configuration files, or any software installed on the device. Modifications include deletions, changes, or additions of new software to any part of the device configuration. The configuration of each system must be checked against the official master image database to verify any changes to secure configurations that would impact security. This includes both operating system and configuration files. Any of these changes to a device must be detected within 24 hours and notification performed by alerting or sending e-mail notification to a list of enterprise personnel. If possible, devices must prevent changes to the system and send an alert indicating the change was not successful. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until it is investigated and/or remediated.

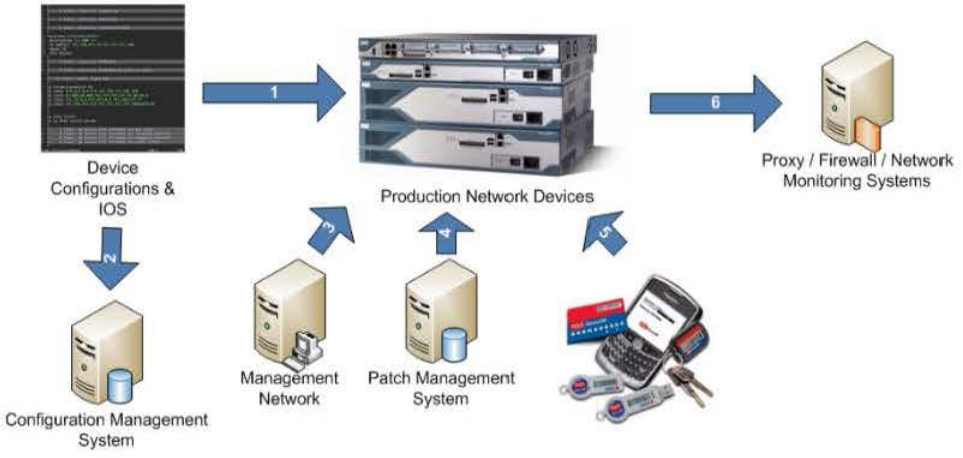
Control 10 Test

To evaluate the implementation of Control 10 on a periodic basis, an evaluation team must make a change to each type of network device plugged into the network. At a minimum, routers, switches, and firewalls need to be tested. If they exist, IPS, IDS, and other network devices must be included. Backups must be made prior to making any changes to critical network devices. It is critical that changes not impact or weaken the security of the device. Acceptable changes include but are not limited to making a comment or adding a duplicate entry in the configuration. The change must be performed twice for each critical device. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the changes to the device within 24 hours. It is important that the evaluation team verify that all unauthorized changes have been detected and have resulted in an alert or e-mail notification. The evaluation team must verify that the system provides details of the location of each device, including information about the asset owner. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting and isolation, with notification about unauthorized configuration changes in network devices sent within two minutes.

If appropriate, an additional test must be performed on a daily basis to ensure that other protocols such as IPv6 are properly being filtered.

Control 10 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case we are examining the network devices, test lab network devices, configuration systems, and configuration management devices. The following list of the steps in the diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify each step in order to help identify potential failure points in the overall control.

Step 1: Hardened device configurations applied to production devices

Step 2: Hardened device configuration stored in a secure configuration management system

Step 3: Management network system validates configurations on production network devices

Step 4: Patch management system applies tested software updates to production network devices

Step 5: Two-factor authentication system required for administrative access to production devices

Step 6: Proxy/firewall/network monitoring systems analyzes all connections to production network devices

Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services

The processes and tools used to track/control/prevent/correct use of ports, protocols, and services on networked devices.

How Do Attackers Exploit the Absence of this Control?

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Any service that is not needed should be turned off for 30 days and after 30 days uninstalled from the system.
2. *Quick wins:* Host-based firewalls or port filtering tools should be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
3. *Quick wins:* Automated port scans should be performed on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.
4. *Quick wins:* All services should be kept up to date and any unnecessary components uninstalled and removed from the system.
5. *Visibility/Attribution:* Any server that is visible from the Internet or an untrusted network should be verified, and if it is not required for business purposes, it should be moved to an internal VLAN and given a private address.
6. *Configuration/Hygiene:* Services needed for business use across the internal network should be reviewed quarterly via a change control group, and business units should rejustify the business use. Services that are turned on for projects or limited engagements should be turned off when they are no longer needed and properly documented.
7. *Configuration/Hygiene:* Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
8. *Advanced:* Application firewalls should be placed in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 3: Network Architecture
Security Gateways, Proxies, and Firewalls

Procedures and Tools to Implement and Automate this Control

Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered open port. This list of services and their versions are compared against an inventory of services required by the organization for each server and workstation in an asset management system. Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

Control 11 Metric

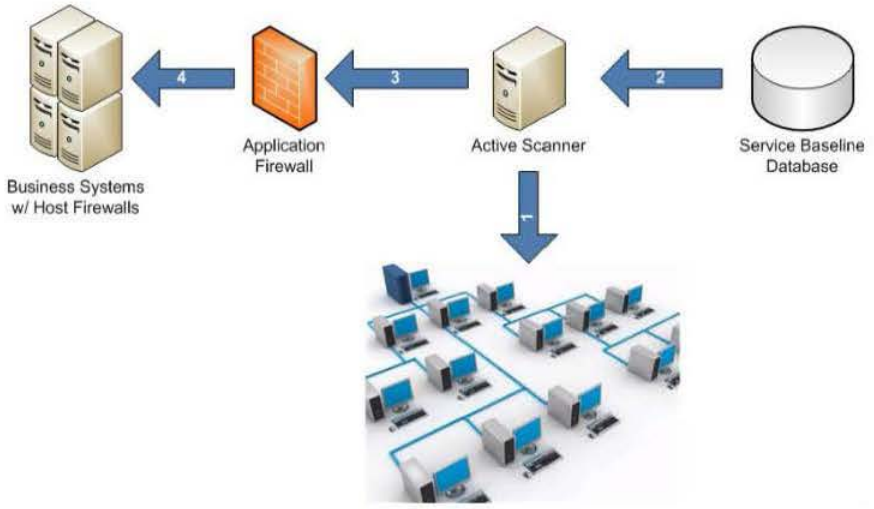
The system must be capable of identifying any new unauthorized listening network ports that are connected to the network within 24 hours, alerting or sending e-mail notification to a list of enterprise personnel. Every 24 hours after that point, the system must alert or send e-mail about the status of the system until the listening network port has been disabled or has been authorized by change management. The system service baseline database and alerting system must be able to identify the location, department, and other details about the system where authorized and unauthorized network ports are running. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

Control 11 Test

To evaluate the implementation of Control 11 on a periodic basis, the evaluation team must install hardened test services with network listeners on 10 locations on the network, including a selection of subnets associated with DMZs, workstations, and servers. The selection of these systems must be as random as possible and include a cross-section of the organization's systems and locations. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the newly installed services within 24 hours of the services being installed on the network. The team must verify that the system provides details of the location of all of the systems where test services have been installed.

Control 11 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining how active scanning systems gather information on network devices and evaluate that data against the authorized service baseline database. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Active scanner analyzes production systems for unauthorized ports, protocols, and services

Step 2: System baselines regularly updated based on necessary/required services

Step 3: Active scanner validates which ports, protocols and services are blocked or allowed by the application firewall

Step 4: Active scanner validates which ports, protocols and services are accessible on business systems protected with host based firewalls

Critical Control 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

How Do Attackers Exploit the Absence of this Control?

The misuse of administrator privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first common attack technique, a workstation user, running as a privileged user, is fooled into opening a malicious e-mail attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content. If the victim user's account has administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data. Similar attacks occur with e-mail. An administrator inadvertently opens an e-mail that contains an infected attachment and this is used to obtain a pivot point within the network that is used to attack other systems.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
2. *Quick wins:* Configure all administrative passwords to be complex and contain letters, numbers and special characters intermixed with no dictionary words present in the password. Strong passwords should be of a sufficient length to increase the difficultly it takes to crack the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.
3. *Quick wins:* Configure all administrative-level accounts to require regular password changes on a frequent interval tied to the complexity of the password.
4. *Quick wins:* Before deploying any new devices in a networked environment, organizations should change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to a difficult-to-guess value.
5. *Quick wins:* Ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrator passwords, at a frequent interval of no longer than 90 days.
6. *Quick wins:* Passwords for all systems should be stored in a well-hashed or encrypted format, with weaker formats eliminated from the environment. Furthermore, files

containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super-user privileges.

7. *Quick wins:* Utilize access control lists to ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet. Web browsers and e-mail clients especially must be configured to never run as administrator.
8. *Quick wins:* Through policy and user awareness, require that administrators establish unique, different passwords for their administrator and nonadministrator accounts. Each person requiring administrative access should be given his/her own separate account. Administrative accounts should never be shared. Users should only use the Windows "administrator" or Unix "root" accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrator accounts.
9. *Quick wins:* Configure operating systems so that passwords cannot be re-used within a certain timeframe, such as six months.
10. *Visibility/Attribution:* Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior (e.g., system reconfigurations during the night shift).
11. *Visibility/Attribution:* Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators group.
12. *Configuration/Hygiene:* All administrative access, including domain administrative access, should use two-factor authentication.
13. *Configuration/Hygiene:* Access to a machine (either remotely or locally) should be blocked for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and nonadministrative account. Then, once logged in to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrator accounts and enter a password each time that is different that their user account.
14. *Configuration/Hygiene:* If services are outsourced to third parties, language should be included in the contracts to ensure that they properly protect and control administrative access. It should be validated that they are not sharing passwords and have accountability to hold administrators liable for their actions.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 5: User Access
Milestone 7: Baseline Management

Procedures and Tools to Implement and Automate this Control

Built-in operating system features can extract lists of accounts with super-user privileges, both locally on individual systems and on overall domain controllers. To verify that users with high-privileged accounts do not use such accounts for day-to-day web surfing and e-mail reading, security personnel should periodically gather a list of running processes to determine whether any browsers or e-mail readers are running with high privileges. Such information gathering can be scripted, with short shell scripts searching for a dozen or more different browsers, e-mail readers, and document editing programs running with high privileges on machines. Some legitimate system administration activity may require the execution of such programs over the short term, but long-term or frequent use of such programs with administrative privileges could indicate that an administrator is not adhering to this control.

To enforce the requirement for strong passwords, built-in operating system features for minimum password length can be configured that prevent users from choosing short passwords. To enforce password complexity (requiring passwords to be a string of pseudo-random characters), built-in operating system settings or third-party password complexity enforcement tools can be applied.

Control 12 Metric

The system must be configured to comply with password policies at least as stringent as those described in the controls above. Additionally, security personnel must be notified via an alert or e-mail within 24 hours of the addition of an account to a super-user group, such as a domain administrator. Every 24 hours after that point, the system must alert or send e-mail about the status of administrative privileges until the unauthorized change has been corrected or authorized through a change management process. While the 24-hour timeframes represent the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

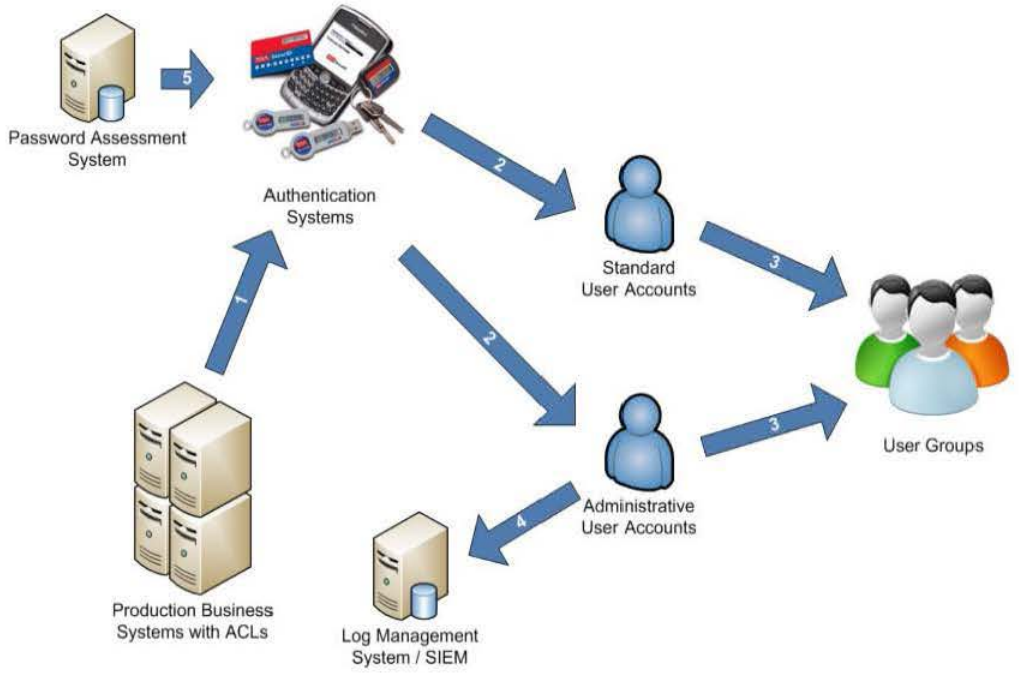
Control 12 Test

To evaluate the implementation of Control 12 on a periodic basis, an evaluation team must verify that the organization's password policy is enforced by creating a temporary, disabled, limited privilege test account on 10 different systems and then attempting to change the password on the account to a value that does not meet the organization's password policy. The selection of these systems must be as random as possible and include a cross-section of the organization's systems and locations. After completion of the test, this account must be removed. Furthermore, the evaluation team must add a temporary disabled test account to a super-user group (such as a domain administrator group) to verify that an alert or e-mail is generated within 24 hours. After this test, the account must be removed from the group and disabled.

Finally, on a periodic basis, the evaluation team must run a script that determines which browser and e-mail client programs are running on a sample of 10 test systems, including five clients and five servers. Any browsers or mail client software running with Windows administrator or Linux/Unix UID 0 privileges must be identified.

Control 12 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the components of user account provisioning and user authentication. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Production systems use proper authentication systems

Step 2: Standard and administrative user accounts use proper authentication systems

Step 3: Standard and administrative user accounts properly managed via group memberships

Step 4: Administrative access to systems properly logged via log management systems

Step 5: Password assessment system validates the strength of the authentication systems

Critical Control 13: Boundary Defense

The processes and tools used to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

How Do Attackers Exploit the Absence of this Control?

Attackers focus on exploiting systems that they can reach across the Internet, including not only DMZ systems but also workstation and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (white lists). Tests can be periodically carried out by sending packets from bogon source IP addresses (unroutable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.
2. *Quick wins:* On DMZ networks, monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) should be configured to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a

FTC-0002308

properly configured Security Event Information Management (SEIM) or log analytics system so that events can be correlated from all devices on the network.

3. *Quick wins:* To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.
4. *Visibility/Attribution:* Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.
5. *Visibility/Attribution:* Network-based IPS devices should be deployed to compliment IDS by blocking known bad signature or behavior of attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic.
6. *Visibility/Attribution:* Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one proxy on a DMZ network. The proxy should support logging individual TCP sessions; blocking specific URLs, domain names, and IP addresses to implement a black list; and applying white lists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Proxies can also be used to encrypt all traffic leaving an organization.
7. *Visibility/Attribution:* Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
8. *Configuration/Hygiene:* All devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels.
9. *Configuration/Hygiene:* Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.
10. *Configuration/Hygiene:* To limit access by an insider or malware spreading on an internal network, organizations should devise internal network segmentation schemes to limit traffic to only those services needed for business use across the internal network.
11. *Configuration/Hygiene:* Develop plans to rapidly deploy filters on internal networks to help stop the spread of malware or an intruder.
12. *Advanced:* To minimize the impact of an attacker pivoting between compromised systems, only allow DMZ systems to communicate with private network systems via application proxies or application-aware firewalls over approved channels
13. *Advanced:* To help identify covert channels exfiltrating data through a firewall, built-in firewall session tracking mechanisms included in many commercial firewalls should be configured to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.
14. *Advanced:* Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7.

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 3: Network Architecture
Security Gateways, Proxies, and Firewalls
Remote Access Security
Network Security Monitoring

Procedures and Tools to Implement and Automate this Control

The boundary defenses included in this control build on Critical Control 10. The additional recommendations here focus on improving the overall architecture and implementation of both Internet and internal network boundary points. Internal network segmentation is central to this control because once inside a network, many intruders attempt to target the most sensitive machines. Usually, internal network protections are not set up to defend against an internal attacker. Setting up even a basic level of security segmentation across the network and protecting each segment with a proxy and a firewall will greatly reduce an intruder's access to the other parts of the network.

One element of this control can be implemented using free or commercial IDS and sniffers to look for attacks from external sources directed at DMZ and internal systems, as well as attacks originating from internal systems against the DMZ or Internet. Security personnel should regularly test these sensors by launching vulnerability-scanning tools against them to verify that the scanner traffic triggers an appropriate alert. The captured packets of the IDS sensors should be reviewed using an automated script each day to ensure that log volumes are within expected parameters and that the logs are formatted properly and have not been corrupted.

Additionally, packet sniffers should be deployed on DMZs to look for Hypertext Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. By sampling traffic regularly, such as over a three-hour period once per week, information security personnel can search for HTTP traffic that is neither sourced by nor destined for a DMZ proxy, implying that the requirement for proxy use is being bypassed.

To identify back-channel connections that bypass approved DMZs, network security personnel can establish an Internet-accessible system to use as a receiver for testing outbound access. This system is configured with a free or commercial packet sniffer. Then, security personnel can connect a sending test system to various points on the organization's internal network, sending easily identifiable traffic to the sniffing receiver on the Internet. These packets can be generated using free or commercial tools with a payload that contains a custom file used for the test. When the packets arrive at the receiver system, the source address of the packets should be verified against acceptable DMZ addresses allowed for the organization. If source addresses are discovered that are not included in legitimate, registered DMZs, more detail can be gathered by

using a traceroute tool to determine the path that packets take from the sender to the receiver system.

Control 13 Metric

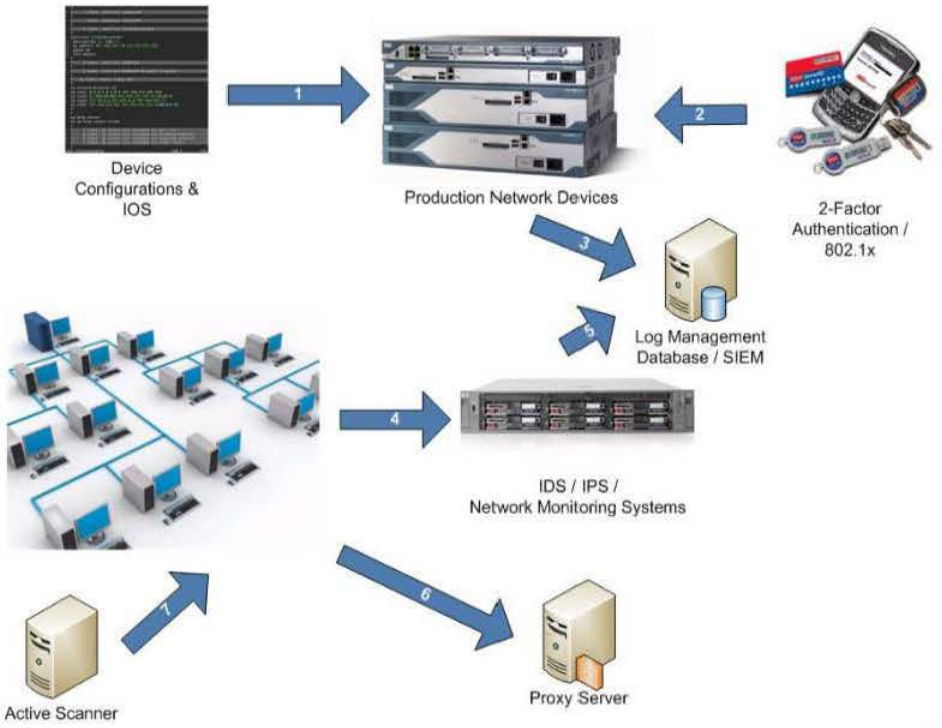
The system must be capable of identifying any unauthorized packets sent into or out of a trusted zone and ensure that the packets are properly blocked and/or trigger alerts. Any unauthorized packets must be detected within 24 hours, with the system generating an alert or e-mail for enterprise administrative personnel. Alerts must be sent every hour thereafter until the boundary device is reconfigured. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

Control 13 Test

To evaluate the implementation of Control 13 on a periodic basis, an evaluation team must test boundary devices by sending packets from outside any trusted network to ensure that only authorized packets are allowed through the boundary. All other packets must be dropped. In addition, unauthorized packets must be sent from a trusted network to an untrusted network to make sure egress filtering is functioning properly. The evaluation team must then verify that the systems generate an alert or e-mail notice regarding the unauthorized packets within 24 hours. It is important that the evaluation team verify that all unauthorized packets have been detected. The evaluation team must also verify that the alert or e-mail indicating that the unauthorized traffic is now being blocked is received within one hour. The evaluation team must verify that the system provides details of the location of each machine with this new test software, including information about the asset owner. It is also important that the evaluation team test to ensure that the device fails in a state where it does not forward traffic when it crashes or becomes flooded.

Control 13 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case we are examining the network boundary devices and the supporting systems such as authentication servers, two-factor authentication systems, network monitoring systems, and network proxy devices. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. This also helps identify what each of the steps is in order to help identify potential failure points in the overall control.

Step 1: Hardened device configurations applied to production devices

Step 2: Two-factor authentication systems required for administrative access to production devices

Step 3: Production network devices send events to log management and correlation system

Step 4: Network monitoring system analyzes network traffic

Step 5: Network monitoring system sends events to log management and correlation system

Step 6: Outbound traffic passes through and is examined by network proxy devices

Step 7: Network systems scanned for potential weaknesses.

Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs

The processes and tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization.

How Do Attackers Exploit the Absence of this Control?

Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but attackers rely on the fact that such organizations rarely look at the audit logs, so they do not know that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Each organization should include at least two synchronized time sources (i.e., Network Time Protocol – NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.
2. *Quick wins:* Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.
3. *Quick wins:* Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.
4. *Quick wins:* Develop a log retention policy to make sure that the logs are kept for a sufficient period of time. As APT (advanced persistent threat) continues to stealthily break into systems, organizations are often compromised for several months without detection. The logs must be kept for a longer period of time than it takes an organization to detect an attack so they can accurately determine what occurred.
5. *Quick wins:* All remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism), should be logged verbosely.
6. *Quick wins:* Operating systems should be configured to log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions. Failed logon attempts must also be logged.

7. *Quick wins:* Security personnel and/or system administrators should run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.
8. *Visibility/Attribution:* Network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, should be configured to verbosely log all traffic (both allowed and blocked) arriving at the device.
9. *Visibility/Attribution:* For all servers, organizations should ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from hosts generating the event logs, lowering the chance that an attacker can manipulate logs stored locally on compromised machines.
10. *Visibility/Attribution:* Deploy a SIM/SEM (security incident management/security event management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIM/SEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.
11. *Advanced:* Carefully monitor for service creation events. On Windows systems, many attackers use psexec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Remote Access Security
Log Management

Procedures and Tools to Implement and Automate this Control

Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organization should periodically scan through its logs and compare them with the asset inventory assembled as part of Critical Control 1 in order to ensure that each managed item actively connected to the network is periodically generating logs.

Analytical programs such as SIM/SEM solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, including, importantly, even just

a cursory examination by a person. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

Control 14 Metric

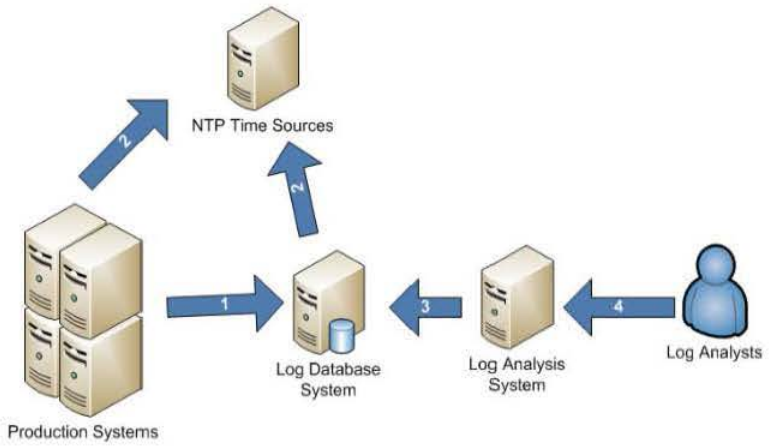
The system must be capable of logging all events across the network. The logging must be validated across both network-based and host-based systems. Any event must generate a log entry that includes a date, timestamp, source address, destination address, and other details about the packet. Any activity performed on the network must be logged immediately to all devices along the critical path. When a device detects that it is not capable of generating logs (due to a log server crash or other issue), it must generate an alert or e-mail for enterprise administrative personnel within 24 hours. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

Control 14 Test

To evaluate the implementation of Control 14 on a periodic basis, an evaluation team must review the security logs of various network devices, servers, and hosts. At a minimum the following devices must be tested: two routers, two firewalls, two switches, 10 servers, and 10 client systems. The testing team should use traffic-generating tools to send packets through the systems under analysis to verify that the traffic is logged. This analysis is done by creating controlled, benign events and determining if the information is properly recorded in the logs with key information, including a date, timestamp, source address, destination address, and other details about the packet. The evaluation team must verify that the system generates audit logs and, if not, an alert or e-mail notice regarding the failed logging must be sent within 24 hours. It is important that the team verify that all activity has been detected. The evaluation team must verify that the system provides details of the location of each machine, including information about the asset owner.

Control 14 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining audit logs, the central log database system, the central time system, and log analysts. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. It also helps identify what each of the steps is in order to help identify potential failure points in the overall control.

Step 1: Production systems generate logs and send them to a centrally managed log database system

Step 2: Production systems and log database system pulls synchronize time with central time management systems

Step 3: Logs analyzed by a log analysis system

Step 4: Log analysts analyze data generated by log analysis system

Critical Control 15: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information based on an approved classification.

How Do Attackers Exploit the Absence of this Control?

Some organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information on their internal networks. In many environments, internal users have access to all or most of the information on the network. Once attackers have penetrated such a network, they can easily find and exfiltrate important information with little resistance. In several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Any sensitive information should be located on separated VLANS with proper firewall filtering. All communication of sensitive information over less-trusted networks needs to be encrypted.
2. *Visibility/Attribution:* Establish a multi-level data identification/classification scheme (e.g., a three- or four-tiered scheme with data separated into categories based on the impact of exposure of the data).
3. *Visibility/Attribution:* Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.
4. *Configuration/Hygiene:* The network should be segmented based on the trust levels of the information stored on the servers. Whenever information flows over a network of lower trust level, the information should be encrypted.
5. *Advanced:* Host-based data loss prevention (DLP) should be used to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6, MP-3, RA-2 (a)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 3: Network Architecture

Procedures and Tools to Implement and Automate this Control

It is important that an organization understand what its sensitive information is, where it resides, and who needs access to it. To derive sensitivity levels, organizations need to put together a list of the key types of data and the overall importance to the organization. This analysis would be used to create an overall data classification scheme for the organization. At a base level, a data classification scheme is broken down into two levels: public (unclassified) and private (classified). Once the private information has been identified, it can then be further subdivided based on the impact it would have to the organization if it were compromised.

Once the sensitivity of the data has been identified, it needs to be traced back to business applications and the physical servers that house those applications. The network then needs to be segmented so that systems of the same sensitivity level are on the same network and segmented from systems of different trust levels. If possible, firewalls need to control access to each segment. If data are flowing over a network of a lower trust level, encryption should be used.

Job requirements should be created for each user group to determine what information the group needs access to in order to perform its jobs. Based on the requirements, access should only be given to the segments or servers that are needed for each job function. Detailed logging should be turned on for all servers so that access can be tracked and situations where someone is accessing data that they should not be accessing can be examined.

Control 15 Metric

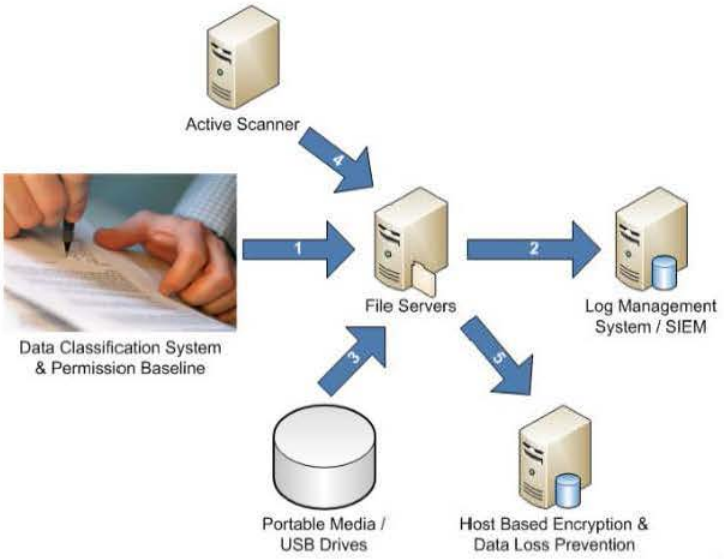
The system must be capable of detecting all attempts by users to access files on local systems or network-accessible file shares without the appropriate privileges, and it must generate an alert or e-mail for administrative personnel within 24 hours. While the 24-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

Control 15 Test

To evaluate the implementation of Control 15 on a periodic basis, the evaluation team must create two test accounts each on 10 representative systems in the enterprise: five server machines and five client systems. For each system evaluated, one account must have limited privileges, while the other must have privileges necessary to create files on the systems. The evaluation team must then verify that the nonprivileged account is unable to access the files created for the other account on the system. The team must also verify that an alert or e-mail is generated based on the attempted unsuccessful access within 24 hours. Upon completion of the test, these accounts must be removed.

Control 15 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, the data classification system and permission baseline is the blueprint for how authentication and access of data is controlled. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: An appropriate data classification system and permissions baseline applied to production data systems

Step 2: Access appropriately logged to a log management system

Step 3: Proper access control applied to portable media/USB drives

Step 4: Active scanner validates, checks access and checks data classification

Step 5: Host based encryption and data loss prevention validates and checks all access requests

Critical Control 16: Account Monitoring and Control

The processes and tools used to track/control/prevent/correct the use of system and application accounts.

How Do Attackers Exploit the Absence of this Control?

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Review all system accounts and disable any account that cannot be associated with a business process and owner.
2. *Quick wins:* All accounts should have an expiration date associated with the account.
3. *Quick wins:* Systems should automatically create a report on a daily basis that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list should be sent to the associated system administrator in a secure fashion.
4. *Quick wins:* Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.
5. *Quick wins:* Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
6. *Quick wins:* Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy. After a longer period, such as 60 days, the account should be disabled.
7. *Quick wins:* When a dormant account is disabled, any files associated with that account should be encrypted and moved to a secure file server for analysis by security or management personnel.
8. *Quick wins:* All nonadministrator accounts should be required to have strong passwords that contain letters, numbers, and special characters, be changed at least every 90 days, have a minimal age of one day, and not be allowed to use the previous 15 passwords as a new password. These values can be adjusted based on the specific business needs of the organization.
9. *Quick wins:* Account lockout should be used and configured such that after a set number of failed login attempts the account is locked for a standard period of time.
10. *Visibility/Attribution:* On a periodic basis, such as quarterly or at least annually, organizations should require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to active employees or contractors.
11. *Visibility/Attribution:* Monitor attempts to access deactivated accounts through audit logging.

12. *Configuration/Hygiene:* Profile each user's typical account usage by determining normal time-of-day access and access duration for each user. Daily reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration by 150 percent. This includes flagging the use of user's credentials from a computer other than computers usually used by the user.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-2 (e, f, g, h, j, 2, 3, 4, 5), AC-3

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Milestone 5: User Access

Procedures and Tools to Implement and Automate this Control

Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Even when such features are present and active, they often do not provide fine-grained detail about access to the system by default. Security personnel can configure systems to record more detailed information about account access, and use home-grown scripts or third-party log analysis tools to analyze this information and profile user access of various systems.

Accounts must also be tracked very closely. Any account that is dormant must be disabled and eventually removed from the system. All active accounts must be traced back to authorized users of the system and it must be ensured that their passwords are robust and changed on a regular basis. Users must also be logged out of the system after a period of no activity to minimize the possibility of an attacker using their system to extract information from the organization.

Control 16 Metric

The system must be capable of identifying unauthorized user accounts when they exist on the system. An automated list of user accounts on the system must be created every 24 hours and an alert or e-mail must be sent to administrative personnel within one hour of completion of a list being created. While the one-hour timeframe represents the current metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

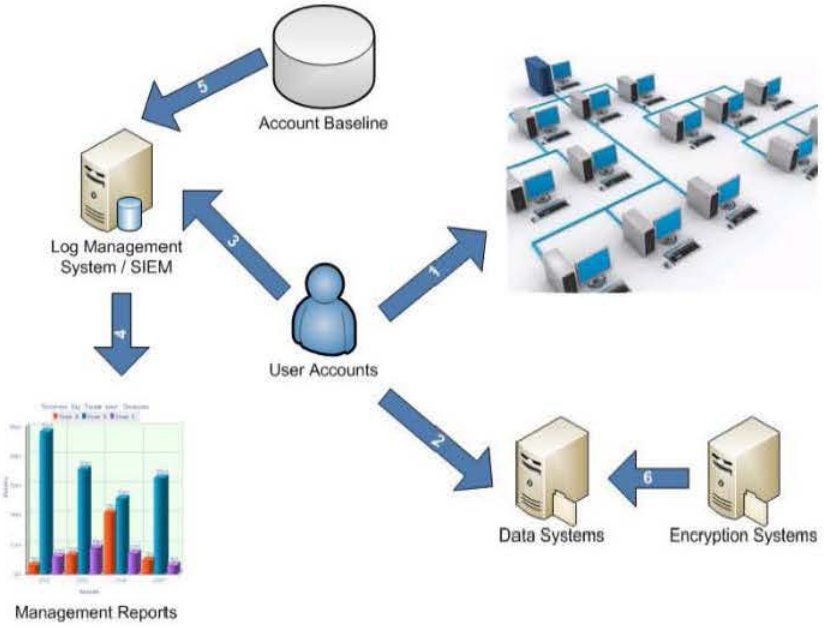
Control 16 Test

To evaluate the implementation of Control 16 on a periodic basis, the evaluation team must verify that the list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire has successfully been completed on a daily basis for the previous 30 days by reviewing archived alerts and reports to ensure that the lists were completed. In addition, a comparison of a baseline

of allowed accounts must be compared to the accounts that are active in all systems. The report of all differences must be created based on this comparison.

Control System 16 Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining user accounts and how they interact with the data systems and the log management systems. Another key component of these systems is the reports generated for management of user accounts.

The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. It also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: User accounts are properly managed on production systems

Step 2: User accounts are assigned proper permissions to production data sets

Step 3: User account access is logged to log management system

Step 4: Log management systems generate user account and access reports for management

Step 5: Account baseline information is sent to log management system

Step 6: Critical information is properly protected and encrypted for each user account

Critical Control 17: Data Loss Prevention

The processes and tools used to track/control/prevent/correct data transmission and storage, based on the data's content and associated classification.

How Do Attackers Exploit the Absence of this Control?

In recent years, attackers have exfiltrated significant amounts of often-sensitive data from organizations of all shapes and sizes. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet in most cases, the victims were not aware that the sensitive data was leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error. Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

The phrase "data loss prevention" refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. Data loss prevention (DLP) controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
2. *Visibility/Attribution:* Deploy an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.
3. *Visibility/Attribution:* Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.

4. *Configuration/Hygiene:* Data should be moved between networks using secure, authenticated, and encrypted mechanisms.
5. *Configuration/Hygiene:* If there is no business need for supporting such devices, organizations should configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.
6. *Configuration/Hygiene:* Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.
7. *Advanced:* Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that organizations be able to detect rogue connections, terminate the connection, and remediate the infected system.
8. *Advanced:* Block access to known file transfer and e-mail exfiltration websites.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

AC-4, MP-2 (2), MP-4 (1), SC-7 (6, 10), SC-9, SC-13, SC-28 (1), SI-4 (4, 11), PM-7

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

Personal Electronic Device (PED) Management
Data-at-Rest Protection
Network Security Monitoring

Procedures and Tools to Implement and Automate this Control

Commercial DLP solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. Organizations deploying such tools should carefully inspect their logs and follow up on any discovered attempts, even those that are successfully blocked, to transmit sensitive information out of the organization without authorization.

Control 17 Metric

The system must be capable of identifying unauthorized data leaving the organization, whether via network file transfers or removable media. Within one hour of a data exfiltration event or attempt, enterprise administrative personnel must be alerted by the appropriate monitoring system. Once the alert has been generated it must also note the system and location where the event or attempt occurred. If the system is in the organization's asset management database, the system owner must also be included in the generated alerts. Every 24 hours after that point, the system must alert or send e-mail about the status of the systems until the source of the event has been identified and the risk mitigated. While the one-hour timeframe represents the current

metric to help organizations improve their state of security, in the future organizations should strive for even more rapid alerting.

Control 17 Test

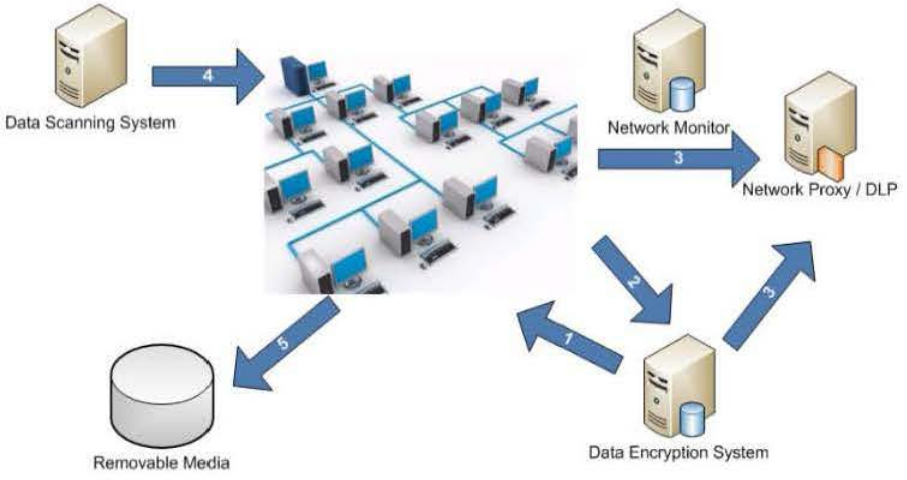
To evaluate the implementation of Control 17 on a periodic basis, the evaluation team must attempt to move test data sets that trigger DLP systems but do not contain sensitive data outside of the trusted computing environment via both network file transfers and removable media. Each of the following tests must be performed at least three times:

- Attempt to transfer large data sets across network boundaries from an internal system.
- Attempt to transfer test data sets of personally identifiable information (that trigger DLP systems but do not contain sensitive data) across network boundaries from an internal system (using multiple keywords specific to the business).
- Attempt to maintain a persistent network connection for at least 10 hours across network boundaries between an internal and external system, even though little data may be exchanged.
- Attempt to maintain a network connection across network boundaries using an anomalous service port number between an internal and external system.
- Insert a USB token into an organization system and attempt to transfer example test data to the USB device.

Each of these tests must be performed from multiple, widely distributed systems on the organization's network in order to test the effectiveness of the monitoring systems. Once each of these events has occurred, the time it takes for enterprise staff to respond to the event must be recorded.

Control System 17 Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the flow of information in and out of the organization in an attempt to limit potential data loss via network or removable media sources. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. It also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Data encryption system ensures that appropriate hard disks are encrypted

Step 2: Sensitive network traffic encrypted

Step 3: Data connections monitored at the network's perimeter by monitoring systems

Step 4: Stored data scanned to identify where sensitive information is stored

Step 5: Offline media encrypted

Critical Control 18: Incident Response and Management

The process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events.

Note: This control has one or more sub-controls that must be validated manually.

How Do Attackers Exploit the Absence of this Control?

Considerable damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully effective incident response plans in place. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow proper procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrating more sensitive data than would otherwise be possible were an effective incident response plan in place.

NIST Special Publication 800-61 contains detailed guidelines for creating and running an incident response team.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
2. *Quick wins:* Assign job titles and duties for handling computer and network incidents to specific individuals.
3. *Quick wins:* Define management personnel who will support the incident handling process by acting in key decision-making roles.
4. *Quick wins:* Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.
5. *Quick wins:* Assemble and maintain information on third party contact information to be used to report a security incident (i.e., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).
6. *Quick wins:* Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
7. *Configuration/Hygiene:* Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

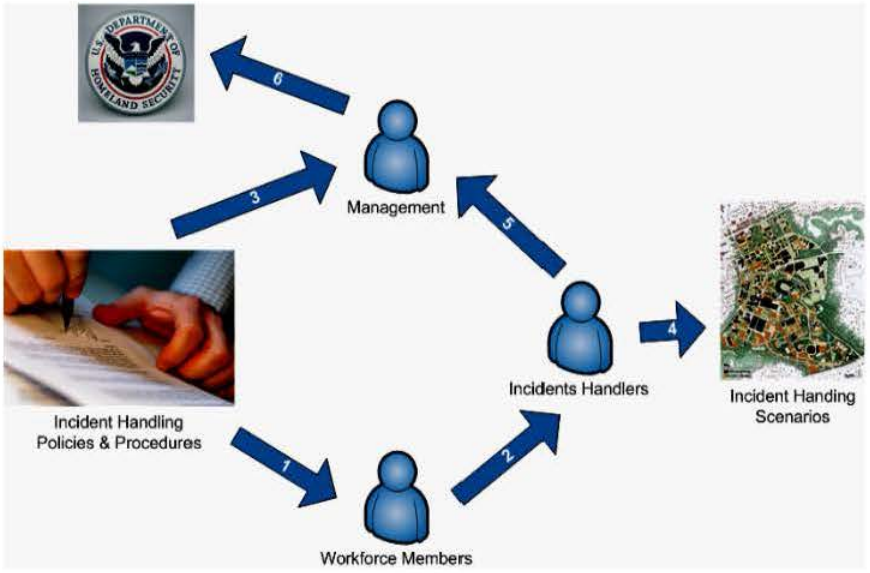
Incident Response and Disaster Recovery Plans
Training

Procedures and Tools to Implement and Automate this Control

After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities the organization faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents.

Control 18 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the incident handling process and how prepared organizations are in the event that an incident occurs. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Incident handling policies and procedures educate workforce members as to their responsibilities during an incident

Step 2: Some workforce members designated as incident handlers

Step 3: Incident handling policies and procedures educate management as to their responsibilities during an incident

Step 4: Incident handlers participate in incident handling scenario tests

Step 5: Incident handlers report incidents to management

Step 6: Organization's management reports incidents to outside law enforcement and the appropriate computer emergency response team (CERT), if necessary

Critical Control 19: Secure Network Engineering

The process and tools used to build, update, and validate a network infrastructure that can properly withstand attacks from advanced threats.

Note: This control has one or more sub-controls that must be validated manually.

How Do Attackers Exploit the Absence of this Control?

Many controls in this document are effective but can be circumvented in networks that are poorly designed. Without a carefully planned and properly implemented network architecture, attackers can bypass security controls on certain systems, pivoting through the network to gain access to target machines. Attackers frequently map networks looking for unneeded connections between systems, weak filtering, and a lack of network separation. Therefore, a robust, secure network engineering process must be employed to complement the detailed controls being measured in other sections of this document.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* The network should be designed using a minimum of a three-tier architecture (DMZ, middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet. DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier.
2. *Configuration/Hygiene:* To support rapid response and shunning of detected attacks, the network architecture and the systems that make it up should be engineered for rapid deployment of new access control lists, rules, signatures, blocks, blackholes, and other defensive measures.
3. *Visibility/Attribution:* DNS should be deployed in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet.
4. *Configuration/Hygiene:* Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

IR-4 (2), SA-8, SC-7 (1, 13), SC-20, SC-21, SC-22, PM-7

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

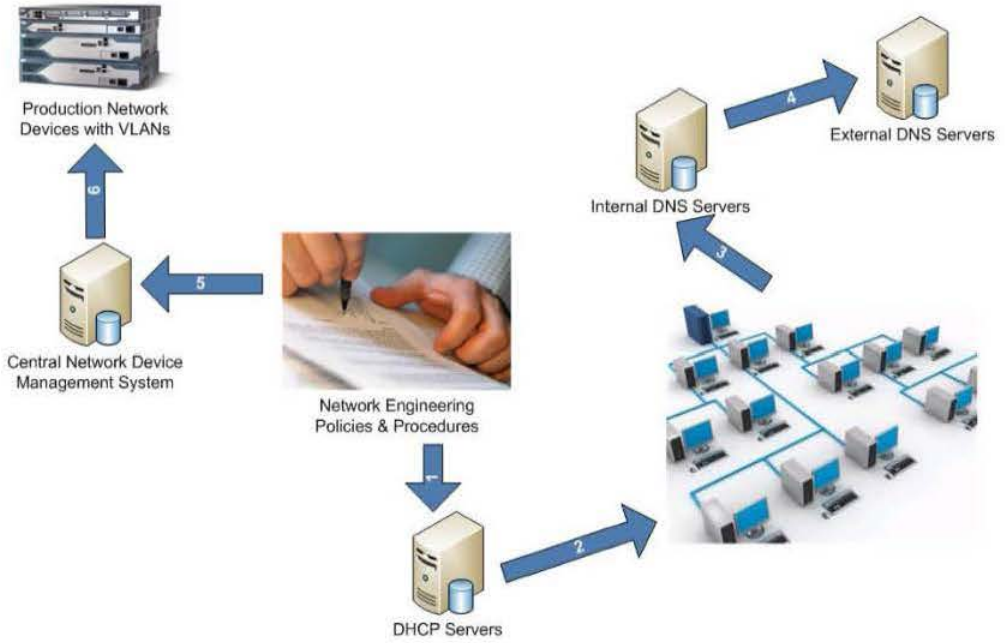
Milestone 3: Network Architecture

Procedures and Tools to Implement and Automate this Control

To help ensure a consistent, defensible network, the architecture of each network should be based on a template that describes the network's overall layout and the services it provides. Organizations should prepare diagrams for each of their networks that show network components such as routers, firewalls, and switches, along with significant servers and groups of client machines.

Control System 19 Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining the network engineering process and evaluating the controls that work together in order to create a secure and robust network architecture. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Network engineering policies and procedures dictate how network systems function to include DHCP (dynamic host configuration protocol) servers

Step 2: DHCP servers provide IP addresses to systems on the network

Step 3: Network devices perform DNS lookups to internal DNS servers

Step 4: Internal DNS servers perform DNS lookups to external DNS servers

Step 5: Network engineering policies and procedures dictate how a central network management system functions

Step 6: Central network management systems configure network devices

Critical Control 20: Penetration Tests and Red Team Exercises

The process and tools used to simulate attacks against a network to validate the overall security of an organization.

Note: This control has one or more sub-controls that must be validated manually.

How Do Attackers Exploit the Absence of this Control?

Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Once they get access, they often burrow deep into target systems and broadly expand the number of machines over which they have control. Most organizations do not exercise their defenses, so they are uncertain about their capabilities and unprepared for identifying and responding to attack.

Penetration testing involves mimicking the actions of computer attackers to identify vulnerabilities in a target organization, and exploiting them to determine what kind of access an attacker can gain. Penetration tests typically provide a deeper analysis of security flaws than a vulnerability assessment. Vulnerability assessments focus on identifying potential vulnerabilities, while penetration testing goes deeper with controlled attempts at exploiting vulnerabilities, approaching target systems as an attacker would. The result provides deeper insight into the business risks of various vulnerabilities by showing whether and how an attacker can compromise machines, pivot to other systems inside a target organization, and gain access to sensitive information.

Red team exercises go further than penetration testing. Red team exercises have the goals of improved readiness of the organization, better training for defensive practitioners, and inspection of current performance levels. Independent red teams can provide valuable and objective insights about the existence of vulnerabilities and about the efficacy of defenses and mitigating controls already in place and even those planned for future implementation.

How to Implement, Automate, and Measure the Effectiveness of this Control

1. *Quick wins:* Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.
2. *Quick wins:* If any user or system accounts are used to perform penetration testing, those accounts should be carefully controlled and monitored to make sure they are only being used for legitimate purposes.
3. *Visibility/Attribution:* Perform periodic red team exercises to test the readiness of organizations to identify and stop attacks or to respond quickly and effectively.
4. *Visibility/Attribution:* Ensure that systemic problems discovered in penetration tests and red team exercises are fully tracked and mitigated.
5. *Visibility/Attribution:* Measure how well the organization has reduced the significant enablers for attackers by setting up automated processes to find:

- Cleartext e-mails and documents with "password" in the filename or body.
- Critical network diagrams stored online and in cleartext.
- Critical configuration files stored online and in cleartext.
- Vulnerability assessment, penetration test reports, and red team finding documents stored online and in cleartext.
- Other sensitive information identified by management personnel as critical to the operation of the enterprise during the scoping of a penetration test or red team exercise.

6. *Visibility/Attribution:* Social engineering should be included within a penetration test. The human element is often the weakest link in an organization and one that attackers often target.
7. *Visibility/Attribution:* Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors, often social engineering combined with web or network exploitation. Red team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.
8. *Configuration/Hygiene:* Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
9. *Advanced:* Devise a scoring method for determining the results of red team exercises so that results can be compared over time.
10. *Advanced:* Create a test bed that mimics a production environment for specific penetration tests and red team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls

CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)

Associated NSA Manageable Network Plan Milestones and Network Security Tasks

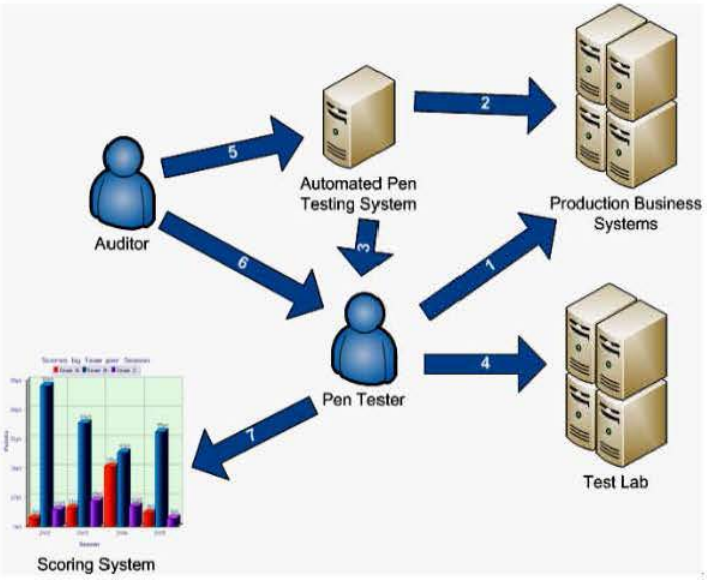
Milestone 3: Network Architecture

Procedures and Tools to Implement and Automate this Control

Each organization should define a clear scope and rules of engagement for penetration testing and red team analyses. The scope of such projects should include, at a minimum, systems with the highest value information and production processing functionality of the organization. Other lowered value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets. The rules of engagement for penetration tests and red team analyses should describe, at a minimum, times of day for testing, duration of tests, and overall test approach.

Control 20 System Entity Relationship Diagram (ERD)

Organizations will find that by diagramming the entities necessary to fully meet the goals defined in this control, it will be easier to identify how to implement them, test the controls, and identify where potential failures in the system might occur.



A control system is a device or set of devices used to manage, command, direct, or regulate the behavior of other devices or systems. In this case, we are examining red team and penetration exercises and how those efforts can be valuable to enterprise personnel when identifying which vulnerabilities are present in the organization. The following list of the steps in the above diagram shows how the entities work together to meet the business goal defined in this control. The list also helps identify what each of the process steps is in order to help identify potential failure points in the overall control.

Step 1: Penetration testers perform penetration tests of production systems

Step 2: Automated pen-testing tools perform penetration tests of production systems

Step 3: Automated pen-testing tools inform penetration tester of vulnerabilities discovered

Step 4: Penetration testers perform more extensive penetration tests of test lab systems

Step 5: Auditors evaluate and inspect the work performed by automated pen-testing tools

Step 6: Auditors evaluate and inspect the work performed by penetration testers.

Step 7: Penetration testers generate reports and statistics about the vulnerabilities that have been discovered

Summary and Action Plan

This document has been developed through the collaboration of a diverse set of security experts. While there is no such thing as absolute protection, proper implementation of the security controls identified in this document will ensure that an organization is protecting itself against the most significant attacks. As attacks change, additional controls or tools become available, or the state of common security practice advances, this document will continue to be updated to reflect what is viewed by the collaborating authors as the most important security controls to defend against cyber attacks.

Action Plan

Given that these critical controls so closely track current threats and attacks, we recommend that CIOs and CISOs consider several immediate actions to ensure the effectiveness of their security programs:

1) Conduct a gap assessment to compare the organization's current security stance to the detailed recommendations of the critical controls

2) Implement the "quick win" critical controls to address the gaps identified by the assessment over the next one or two quarters

3) Assign security personnel to analyze and understand how critical controls beyond the quick wins can be deployed in the organization's environment

4) Devise detailed plans to implement the "visibility and attribution" and "hardened configuration and improved information security hygiene" critical controls over the next year

5) Plan for deployment of the "advanced controls" over the longer term

FTC-0002337

Appendix A: Mapping between the Critical Security Controls and National Institute of Standards and Technology Special Publication 800-53, Revision 3, Priority 1 Items

This mapping relates the controls set forth in this document to NIST Special Publication 800-53 Revision 3. Please note that the NIST controls may impose additional requirements beyond those explicitly stated in this document.

Control	References
Critical Control 1: Inventory of Authorized and Unauthorized Devices	CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6
Critical Control 2: Inventory of Authorized and Unauthorized Software	CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7
Critical Control 3: Secure Configurations for Hardware and Software	CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
Critical Control 4: Continuous Vulnerability Assessment and Remediation	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)
Critical Control 5: Malware Defenses	SC-18, SC-26, SI-3 (a, b, 1, 2, 5, 6)
Critical Control 6: Application Software Security	CM-7, RA-5 (a, 1), SA-3, SA-4 (3), SA-8, SI-3, SI-10
Critical Control 7: Wireless Device Control	AC-17, AC-18 (1, 2, 3, 4), SC-9 (1), SC-24, SI-4 (14, 15)
Critical Control 8: Data Recovery Capability	CP-9 (a, b, d, 1, 3), CP-10 (6)
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1, AT-2 (1), AT-3 (1)
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	AC-4 (7, 10, 11, 16), CM-1, CM-2 (1), CM-3 (2), CM-5 (1, 2, 5), CM-6 (4), CM-7 (1, 3), IA-2 (1, 6), IA-5, IA-8, RA-5, SC-7 (2, 4, 5, 6, 8, 11, 13, 14, 18), SC-9
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	CM-6 (a, b, d, 2, 3), CM-7 (1), SC-7 (4, 5, 11, 12)
Critical Control 12: Controlled Use of Administrative Privileges	AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)
Critical Control 13: Boundary Defense	AC-17 (1), AC-20, CA-3, IA-2 (1, 2), IA-8, RA-5, SC-7 (1, 2, 3, 8, 10, 11, 14), SC-18, SI-4 (c, 1, 4, 5, 11), PM-7
Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2),

	AU-12 (2), SI-4 (8)
Critical Control 15: Controlled Access Based on the Need to Know	AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6, MP-3, RA-2 (a)
Critical Control 16: Account Monitoring and Control	AC-2 (e, f, g, h, j, 2, 3, 4, 5), AC-3
Critical Control 17: Data Loss Prevention	AC-4, MP-2 (2), MP-4 (1), SC-7 (6, 10), SC-9, SC-13, SC-28 (1), SI-4 (4, 11), PM-7
Critical Control 18: Incident Response Capability	IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8
Critical Control 19: Secure Network Engineering	IR-4 (2), SA-8, SC-7 (1, 13), SC-20, SC-21, SC-22, PM-7,
Critical Control 20: Penetration Tests and Red Team Exercises	CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)

Appendix B: Attack Types

As described in the Introduction, numerous contributors who are responsible for responding to actual attacks or conducting red team exercises were involved in the creation of this document. The resulting controls are therefore based on first-hand knowledge or real-world attacks and the associated defenses.

Attack Summary	Most Directly Related Control
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	1
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploits unpatched and improperly secured client software running on victim machines.	2, 3
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.	2, 4
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.	2, 10
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.	3, 10
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.	4, 5
Attackers compromise target organizations that do not exercise their defenses to determine and continually improve their effectiveness.	4, 5, 11, 20
Attackers use malicious code to gain and maintain control of target machines, capture sensitive data, and then spread it to other systems, sometimes wielding code that disables or dodges signature-based anti-virus tools.	5, 15, 17
Attackers scan for remotely accessible services on target systems that are often unneeded for business activities, but provide an avenue of attack and compromise	5, 10, 11

of the organization.	
Attackers exploit weak application software, particularly web applications, through attack vectors such as SQL injection, cross-site scripting, and similar tools.	6, 20
Attackers exploit wireless access points to gain entry into a target organization's internal network, and exploit wireless client systems to steal sensitive information.	7
Attackers exploit users and system administrators via social engineering scams that work because of a lack of security skills and awareness.	9, 12, 16
Attackers exploit and infiltrate through network devices whose security configuration has been weakened over time by granting, for specific short-term business needs, supposedly temporary exceptions that are never removed.	10, 13
Attackers trick a user with an administrator-level account into opening a phishing-style e-mail with an attachment or surfing to the attacker's content on an Internet website, allowing the attacker's malicious code or exploit to run on the victim machine with full administrator privileges.	9, 12
Attackers exploit boundary systems on Internet-accessible DMZ networks, and then pivot to gain deeper access on internal networks.	13, 19
Attackers exploit poorly designed network architectures by locating unneeded or unprotected connections, weak filtering, or a lack of separation of important systems or business functions.	13, 19
Attackers operate undetected for extended periods of time on compromised systems because of a lack of logging and log review.	14
Attackers gain access to sensitive documents in an organization that does not properly identify and protect sensitive information or separate it from nonsensitive information.	15, 17
Attackers compromise inactive user accounts left behind by temporary workers, contractors, and former employees, including accounts left behind by the attackers themselves who are former employees.	16

Attackers escalate their privileges on victim machines by launching password guessing, password cracking, or privilege escalation exploits to gain administrator control of systems, which is then used to propagate to other victim machines across an enterprise.	12, 16
Attackers gain access to internal enterprise systems gather and exfiltrate sensitive information without detection by the victim organization.	17
Attackers compromise systems and alter important data, potentially jeopardizing organizational effectiveness via polluted information.	15, 17
Attackers operate undiscovered in organizations without effective incident-response capabilities, and when they are discovered, such organizations often cannot properly contain the attack, eradicate the attacker's presence, or recover to a secure production state.	18

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 7
TO EXPERT REPORT OF DR. ERIC B. COLE

Security Standards Council ™

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 2.0

October 2010

Document Changes

Date	Version	Description	Pages
October 2008	*1.2*	*To introduce PCI DSS v1.2 as "PCI DSS Requirements and Security Assessment Procedures," eliminating redundancy between documents, and make both general and specific changes from* PCI DSS Security Audit Procedures v1.1. *For complete information, see* PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2.	
July 2009	*1.2.1*	*Add sentence that was incorrectly deleted between PCI DSS v1.1 and v1.2.*	*5*
		Correct "then" to "than" in testing procedures 6.3.7.a and 6.3.7.b.	*32*
		Remove grayed-out marking for "in place" and "not in place" columns in testing procedure 6.5.b.	*33*
		For Compensating Controls Worksheet – Completed Example, correct wording at top of page to say "Use this worksheet to define compensating controls for any requirement noted as 'in place' via compensating controls."	*64*
October 2010	*2.0*	*Update and implement changes from v1.2.1. For details, please see* "PCI DSS - Summary of Changes from PCI DSS Version 1.2.1 to 2.0."	

FTC-0002095

Copyright 2010 PCI Security Standards Council LLC

Table of Contents

Document Changes **2**
Introduction and PCI Data Security Standard Overview **5**
PCI DSS Applicability Information **7**
Relationship between PCI DSS and PA-DSS **9**
Scope of Assessment for Compliance with PCI DSS Requirements **10**
Network Segmentation *10*
Wireless *11*
Third Parties/Outsourcing *11*
Sampling of Business Facilities/System Components *12*
Compensating Controls *13*
Instructions and Content for Report on Compliance **14**
Report Content and Format *14*
Revalidation of Open Items *17*
PCI DSS Compliance – Completion Steps *18*
Detailed PCI DSS Requirements and Security Assessment Procedures **19**
Build and Maintain a Secure Network **20**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data *20*
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters *24*
Protect Cardholder Data **28**
Requirement 3: Protect stored cardholder data *28*
Requirement 4: Encrypt transmission of cardholder data across open, public networks *35*
Maintain a Vulnerability Management Program **37**
Requirement 5: Use and regularly update anti-virus software or programs *37*
Requirement 6: Develop and maintain secure systems and applications *38*
Implement Strong Access Control Measures **44**
Requirement 7: Restrict access to cardholder data by business need to know *44*
Requirement 8: Assign a unique ID to each person with computer access *46*
Requirement 9: Restrict physical access to cardholder data *51*
Regularly Monitor and Test Networks **55**
Requirement 10: Track and monitor all access to network resources and cardholder data *55*

FTC-0002096

Copyright 2010 PCI Security Standards Council LLC

Requirement 11: Regularly test security systems and processes. *59*
Maintain an Information Security Policy **64**
Requirement 12: Maintain a policy that addresses information security for all personnel. *64*
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers **70**
Appendix B: Compensating Controls **72**
Appendix C: Compensating Controls Worksheet **73**
Compensating Controls Worksheet – Completed Example **74**
Appendix D: Segmentation and Sampling of Business Facilities/System Components **75**

FTC-0002097

Copyright 2010 PCI Security Standards Council LLC

Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. Below is a high-level overview of the 12 PCI DSS requirements.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Use and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Assign a unique ID to each person with computer access **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes.
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel.

This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process. The following sections provide detailed guidelines and best practices to assist entities prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS Requirements and Testing Procedures begin on **page 19.**

FTC-0002098

Copyright 2010 PCI Security Standards Council LLC

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources, including:

- Attestations of Compliance
- *Navigating PCI DSS: Understanding the Intent of the Requirements*
- The *PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms*
- Frequently Asked Questions (FAQs)
- Information Supplements and Guidelines

Please refer to www.pcisecuritystandards.org for more information.

***Note**: Information Supplements complement the PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements – they do not change, eliminate or supersede the PCI DSS or any of its requirements.*

FTC-0002099

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Applicability Information

PCI DSS applies wherever account data is stored, processed or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data*, as follows:

Cardholder Data includes:	***Sensitive Authentication Data includes:***
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full magnetic stripe data or equivalent on a chip ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

The primary account number is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements ***except*** Requirements 3.3 and 3.4, which apply only to PAN.

PCI DSS represents a minimum set of control objectives which may be enhanced by local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name), or define an entity's disclosure practices related to consumer information. Examples include legislation related to consumer data protection, privacy, identity theft, or data security. PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

The following table illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

FTC-0002100

Copyright 2010 PCI Security Standards Council LLC

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

PCI DSS requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS ***only applies*** if PANs are stored, processed and/or transmitted.

1 *Sensitive authentication data must not be stored after authorization (even if encrypted).*

2 *Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.*

FTC-0002101

Copyright 2010 PCI Security Standards Council LLC

Relationship between PCI DSS and PA-DSS

Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor (per PA-DSS Requirement 13.1).

The requirements for the Payment Application Data Security Standard (PA-DSS) are derived from the *PCI DSS Requirements and Security Assessment Procedures* (this document). The PA-DSS details what a payment application must support to facilitate a customer's PCI DSS compliance.

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card verification codes and values (CAV2, CID, CVC2, CVV2), and PINs and PIN blocks, along with the damaging fraud resulting from these breaches.

Just a few of the ways payment applications can prevent compliance include:

- Storage of magnetic stripe data and/or equivalent data from the chip in the customer's network after authorization;
- Applications that require customers to disable other features required by the PCI DSS, like anti-virus software or firewalls, in order to get the payment application to work properly; and
- Vendors' use of unsecured methods to connect to the application to provide support to the customer.

The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

Please note the following regarding PA-DSS applicability:

- PA-DSS ***does*** apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
- PA-DSS ***does not*** apply to payment applications developed by merchants and service providers if used only in-house (not sold, distributed, or licensed to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For detailed guidance on determining whether PA-DSS applies to a given payment application, please refer to the PA-DSS Requirements and Security Assessment Procedures, which can be found at www.pcisecuritystandards.org.

FTC-0002102

Copyright 2010 PCI Security Standards Council LLC

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. "System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.
- The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.

Network Segmentation

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

FTC-0002103

Copyright 2010 PCI Security Standards Council LLC

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented.

Appendix D: Segmentation and Sampling of Business Facilities/System Components provides more information on the effect of network segmentation and sampling on the scope of a PCI DSS assessment.

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (WLAN) is connected to, or part of, the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Third Parties/Outsourcing

For service providers required to undergo an annual onsite assessment, compliance validation must be performed on all system components in the cardholder data environment.

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance (ROC) must document the role of each service provider, clearly identifying which requirements apply to the assessed entity and which apply to the service provider. There are two options for third-party service providers to validate compliance:

Copyright 2010 PCI Security Standards Council LLC

1) They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance; or
2) If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customers' PCI DSS assessments.

See the bullet beginning "For managed service provider (MSP) reviews," in Item 3, "Details about Reviewed Environment," in the "Instructions and Content for Report on Compliance" section, below, for more information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*

Sampling of Business Facilities/System Components

Sampling is not a PCI DSS requirement. However, after considering the overall scope and complexity of the environment being assessed, the assessor may independently select representative samples of business facilities/system components in order to assess PCI DSS requirements. These samples must be defined first for business facilities and then for system components within each selected business facility. Samples must be a representative selection of all of the types and locations of business facilities, as well as types of system components within selected business facilities. Samples must be sufficiently large to provide the assessor with assurance that controls are implemented as expected.

Sampling of business facilities/system components for an assessment does not reduce the scope of the cardholder data environment or the applicability of PCI DSS requirements. Whether or not sampling is to be used, PCI DSS requirements apply to the entire cardholder data environment. If sampling is used, each sample must be assessed against all applicable PCI DSS requirements. Sampling of the PCI DSS Requirements themselves is not permitted.

Examples of business facilities include but are not limited to: corporate offices, stores, franchise locations, processing facilities, data centers, and other facility types in different locations. Sampling should include system components within each selected business facility. For example, for each business facility selected, include a variety of operating systems, functions, and applications that are applicable to the area under review.

As an example, the assessor may define a sample at a business facility to include Sun servers running Apache WWW, Windows servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single version of an OS (for example, Windows 7 or Solaris 10), then the sample should still include a variety of applications (for example, database servers, web servers, data transfer servers).

When independently selecting samples of business facilities/system components, assessors should consider the following:

- If there are standard, centralized PCI DSS security and operational processes and controls in place that ensure consistency and that each business facility/system component must follow, the sample can be smaller than if there are no standard processes/controls in place. The sample must be large enough to provide the assessor with reasonable assurance that all business facilities/system components are configured per the standard processes.
- If there is more than one type of standard security and/or operational process in place (for example, for different types of business facilities/system components), the sample must be large enough to include business facilities/system components secured with each type of process.

FTC-0002105

Copyright 2010 PCI Security Standards Council LLC

- If there are no standard PCI DSS processes/controls in place and each business facility/system component is managed through non-standard processes, the sample must be larger for the assessor to be assured that each business facility/system component has implemented PCI DSS requirements appropriately.

For each instance where sampling is used, the assessor must:

- Document the rationale behind the sampling technique and sample size,
- Document and validate the standardized PCI DSS processes and controls used to determine sample size, and
- Explain how the sample is appropriate and representative of the overall population.

Assessors must revalidate the sampling rationale for each assessment. If sampling is to be used, different samples of business facilities and system components must be selected for each assessment.

Please also refer to:
Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission, per *Appendix B: Compensating Controls* and *Appendix C: Compensating Controls Worksheet*.

For each and every compensating control, the Compensating Controls Worksheet *(Appendix C)* **must** be completed. Additionally, compensating control results should be documented in the ROC in the corresponding PCI DSS requirement section.

See the above-mentioned *Appendices B* and *C* for more details on "compensating controls."

FTC-0002106

Copyright 2010 PCI Security Standards Council LLC

Instructions and Content for Report on Compliance

This document must be used as the template for creating the *Report on Compliance*. The assessed entity should follow each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. Contact each payment brand to determine reporting requirements and instructions.

Report Content and Format

Follow these instructions for report content and format when completing a Report on Compliance:

1. **Executive Summary**

   Include the following:

   - Describe the entity's payment card business, including:
     - Their business role with payment cards, which is how and why they store, process, and/or transmit cardholder data

       Note: *This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.*
     - How they process payment (directly, indirectly, etc.)
     - What types of payment channels they serve, such as card-not-present (for example, mail-order-telephone-order (MOTO), e-Commerce), or card-present
     - Any entities that they connect to for payment transmission or processing, including processor relationships
   - A high-level network diagram (either obtained from the entity or created by assessor) of the entity's networking topography that includes:
     - Connections into and out of the network
     - Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
     - Other necessary payment components, as applicable

FTC-0002107

Copyright 2010 PCI Security Standards Council LLC

2. Description of Scope of Work and Approach Taken

Describe the scope, per the Scope of Assessment section of this document, including the following:

- Document how the assessor validated the accuracy of the PCI DSS scope for the assessment, including:
  - The methods or processes used to identify and document all existences of cardholder data
  - How the results were evaluated and documented
  - How the effectiveness and accuracy of the methods used were verified
  - That the assessor validates that the scope of the assessment is accurate and appropriate.
- Environment on which assessment focused (for example, client's Internet access points, internal corporate network, processing connections)
- If network segmentation is in place and was used to reduce scope of the PCI DSS review, briefly explain that segmentation and how assessor validated the effectiveness of the segmentation
- If sampling is used during the assessment, for each sample set selected (of business facilities/system components) document the following:
  - Total population
  - Number sampled
  - Rationale for sample selected
  - Description of the standardized PCI DSS security and operational processes and controls used to determine sample size, and how the processes/controls were validated
  - How the sample is appropriate and representative of the overall population
  - Description of any locations or environments that store, process, or transmit cardholder data that were EXCLUDED from the scope of the review, and why these locations/environments were excluded
- List any wholly-owned entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any international entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any wireless LANs and/or wireless payment applications (for example, POS terminals) that are connected to, or could impact the security of the cardholder data environment, and describe security in place for these wireless environments
- The version of the PCI DSS Requirements and Security Assessment Procedures document used to conduct the assessment

FTC-0002108

Copyright 2010 PCI Security Standards Council LLC

3. Details about Reviewed Environment

Include the following details in this section:

- A diagram of each piece of the communication link, including LAN, WAN or Internet
- Description of cardholder data environment, for example:
  - Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback and other flows as applicable
  - List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.):
    - List all of the elements of stored cardholder data
    - How data is secured
    - How access to data stores are logged
- List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each
- List of service providers and other third parties with which the entity shares cardholder data

  Note: *These entities are subject to PCI DSS Requirement 12.8.*)
- List of third-party payment application products and versions numbers in use, including whether each payment application has been validated according to PA-DSS. Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's *PA-DSS Implementation Guide.*

  Note: *It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.)*
- List of individuals interviewed, their organizations, titles, and topics covered
- List of documentation reviewed
- For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.

FTC-0002109

Copyright 2010 PCI Security Standards Council LLC

4. **Contact Information and Report Date**

   Include:

   - Contact information for merchant or service provider and assessor
   - Timeframe of assessment—specify the duration and the time period over which the assessment occurred
   - Date of report

5. **Quarterly Scan Results**

   - Summarize the four most recent quarterly ASV scan results in the Executive Summary as well as in comments at Requirement 11.2.2.

     Note: *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies:*

     1) The most recent scan result was a passing scan,

     2) The entity has documented policies and procedures requiring quarterly scanning going forward, and

     3) Any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan.

     For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.

   - Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI Approved Scanning Vendors (ASV) Program Guide*.

6. **Findings and Observations**

   Summarize in the Executive Summary any findings that may not fit into the standard Report on Compliance template format.

   All assessors *must:*

   - Use the Detailed PCI DSS Requirements and Security Assessment Procedures template to provide detailed report descriptions and findings on each requirement and sub-requirement.
   - Ensure that all N/A responses are clearly explained.
   - Review and document any compensating controls considered to conclude that a control is in place.

   See "Compensating Controls" section above and *Appendices B* and *C* for more details on compensating controls.

Revalidation of Open Items

A "controls in place" report is required to verify compliance. The report is considered non-compliant if it contains "open items," or items that will be finished at a future date. The merchant/service provider must address these items before validation is completed. After open items are addressed by the merchant/service provider, the assessor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new Report on Compliance, verifying that the cardholder data environment is fully compliant, and submit it consistent with instructions (see below).

FTC-0002110

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Compliance – Completion Steps

1. Complete the Report on Compliance (ROC) according to the section above entitled "Instructions and Content for Report on Compliance."
2. Ensure passing vulnerability scan(s) have been completed by a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of passing scan(s) from the ASV.
3. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety. Attestations of Compliance are available on the PCI SSC website (www.pcisecuritystandards.org).
4. Submit the ROC, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

Copyright 2010 PCI Security Standards Council LLC

Detailed PCI DSS Requirements and Security Assessment Procedures

For the *PCI DSS Requirements and Security Assessment Procedures*, the following defines the table column headings:

- **PCI DSS Requirements** – This column defines the Data Security Standard and lists requirements to achieve PCI DSS compliance; compliance will be validated against these requirements.
- **Testing Procedures** – This column shows processes to be followed by the assessor to validate that PCI DSS requirements are "in place."
- **In Place** – This column must be used by the assessor to provide a brief description of the controls which were validated as "in place" for each requirement, including descriptions of controls found to be in place as a result of compensating controls, or as a result of a requirement being "Not Applicable."

  Note: *This column must not be used for controls that are not yet in place or for open items to be completed at a future date.*
- **Not in Place** – This column must be used by the assessor to provide a brief description of controls that are not in place. Note that a non-compliant report should not be submitted to a payment brand or acquirer unless specifically requested. , For further instructions on non-compliant reports, please refer to the Attestations of Compliance, available on the PCI SSC website (www.pcisecuritystandards.org).
- **Target Date/Comments** – For those controls "Not in Place" the assessor may include a target date that the merchant or service provider expects to have controls "In Place." Any additional notes or comments may be included here as well.

FTC-0002112

Copyright 2010 PCI Security Standards Council LLC

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.			
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks.			
	1.1.2.b Verify that the diagram is kept current.			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.			
	1.1.3.b Verify that the current network diagram is consistent with the firewall configuration standards.			

FTC-0002113

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.			
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	**1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.			
	1.1.5.b Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service.			
1.1.6 Requirement to review firewall and router rule sets at least every six months	**1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.			
	1.1.6.b Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.			
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:			
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	**1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.			
	1.2.1.b Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.			

FTC-0002114

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.2.2 Secure and synchronize router configuration files.	**1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations.			
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.			
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below.			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.			
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ.			
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.			
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	**1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ.			
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized			

FTC-0002115

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	**1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)			
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**1.3.7** Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.			
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* ▪ *Network Address Translation (NAT)* ▪ *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,* ▪ *Removal or filtering of route advertisements for private networks that employ registered addressing,* ▪ *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.8.a** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.			
	1.3.8.b Verify that any disclosure of private IP addresses and routing information to external entities is authorized.			
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active.			
	1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.			

FTC-0002116

Copyright 2010 PCI Security Standards Council LLC

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:			
	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions			
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.			
	2.1.1.c Verify default passwords/passphrases on access points were changed.			
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.			
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.			

FTC-0002117

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: ▪ Center for Internet Security (CIS) ▪ International Organization for Standardization (ISO) ▪ SysAdmin Audit Network Security (SANS) Institute ▪ National Institute of Standards Technology (NIST)	**2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.			
	2.2.b Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.			
	2.2.c Verify that system configuration standards are applied when new systems are configured.			
	2.2.d Verify that system configuration standards include each item below (2.2.1 – 2.2.4).			
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	**2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server.			
	2.2.1.b If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.			

FTC-0002118

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	**2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled.			
	2.2.2.b Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented.			
2.2.3 Configure system security parameters to prevent misuse.	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.			
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.			
	2.2.3.c For a sample of system components, verify that common security parameters are set appropriately.			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.			
	2.2.4.b. Verify enabled functions are documented and support secure configuration.			
	2.2.4.c. Verify that only documented functionality is present on the sampled system components.			

FTC-0002119

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**2.3** For a sample of system components, verify that non-console administrative access is encrypted by performing the following:			
	2.3.a Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested.			
	2.3.b Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally.			
	2.3.c Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography.			
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers*.	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.			

FTC-0002120

Copyright 2010 PCI Security Standards Council LLC

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.	**3.1** Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following:			
3.1.1 Implement a data retention and disposal policy that includes: ▪ Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ▪ Processes for secure deletion of data when no longer needed ▪ Specific retention requirements for cardholder data ▪ A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	**3.1.1.a** Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).			
	3.1.1.b Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.			
	3.1.1.c Verify that policies and procedures include coverage for all storage of cardholder data.			
	3.1.1.d Verify that policies and procedures include at least one of the following: A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.			

FTC-0002121

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	3.1.1.e For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy.			
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: ***Note:*** *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*	**3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured.			
	3.2.b For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable.			
	3.2.c For each item of sensitive authentication data below, perform the following steps:			
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ▪ *The cardholder's name* ▪ *Primary account number (PAN)* ▪ *Expiration date* ▪ *Service code* *To minimize risk, store only these data elements as needed for business.*	**3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			

FTC-0002122

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	**3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). ***Notes:*** ▪ *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.			

FTC-0002123

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads, with the pads being securely stored ▪ Strong cryptography, with associated key-management processes and procedures			
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).			
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.			
	3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.			
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).			
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).			
	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored. ***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*			FTC-0002124

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: ***Note:*** *This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.			
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.			
	3.5.2.b Identify key storage locations to verify that keys are stored in the fewest possible locations and forms.			
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data.			
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.			
	3.6.c Examine the key-management procedures and perform the following:			
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.			
3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.			
3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.			

FTC-0002125

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod.			
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened.			
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.			
	3.6.5.c If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations.			

FTC-0002126

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). ***Note:*** *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	**3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys.			
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.			
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**3.6.8** Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.			

FTC-0002127

Copyright 2010 PCI Security Standards Council LLC

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:* ▪ The Internet ▪ Wireless technologies, ▪ Global System for Mobile communications (GSM) ▪ General Packet Radio Service (GPRS).	**4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:			
	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.			
	4.1.b Verify that only trusted keys and/or certificates are accepted.			
	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.			
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)			
	4.1.e For SSL/TLS implementations: ▪ Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). ▪ Verify that no cardholder data is required when HTTPS does not appear in the URL.			

FTC-0002128

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ***Note:*** *The use of WEP as a security control was prohibited as of 30 June 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.			
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	**4.2.a** Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.			
	4.2.b Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.			

FTC-0002129

Copyright 2010 PCI Security Standards Council LLC

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.			
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).			
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	**5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following:			
	5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.			
	5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.			
	5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.			
	5.2.d For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.			

FTC-0002130

Copyright 2010 PCI Security Standards Council LLC

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: *Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. ***Note:*** *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.			
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.			

FTC-0002131

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. ***Notes:*** ▪ *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.* ▪ *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as "High.".			
	6.2.b Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information.			
6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	**6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards and/or best practices.			
	6.3.b Examine written software development processes to verify that information security is included throughout the life cycle.			
	6.3.c Examine written software development processes to verify that software applications are developed in accordance with PCI DSS.			
	6.3.d From an examination of written software development processes, and interviews of software developers, verify that:			
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	**6.3.1** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers.			

FTC-0002132

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. ***Note:*** *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	**6.3.2.a** Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows: ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release.			
	6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.			
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	**6.4** From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following:			
6.4.1 Separate development/test and production environments	**6.4.1** The development/test environments are separate from the production environment, with access control in place to enforce the separation.			
6.4.2 Separation of duties between development/test and production environments	**6.4.2** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.			
6.4.3 Production data (live PANs) are not used for testing or development	**6.4.3** Production data (live PANs) are not used for testing or development.			
6.4.4 Removal of test data and accounts before production systems become active	**6.4.4** Test data and accounts are removed before a production system becomes active.			

FTC-0002133

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	**6.4.5.a** Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below.			
	6.4.5.b For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:			
6.4.5.1 Documentation of impact.	**6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change.			
6.4.5.2 Documented change approval by authorized parties.	**6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change.			
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	**6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.			
	6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.			
6.4.5.4 Back-out procedures.	**6.4.5.4** Verify that back-out procedures are prepared for each sampled change.			
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:	**6.5.a** Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance.			
	6.5.b Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.			
Note: *The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*	**6.5.c.** Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following:			

FTC-0002134

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)			
6.5.2 Buffer overflow	**6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.)			
6.5.3 Insecure cryptographic storage	**6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws)			
6.5.4 Insecure communications	**6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications)			
6.5.5 Improper error handling	**6.5.5** Improper error handling (Do not leak information via error messages)			
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). ***Note:*** *This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*	**6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2.			
Note: *Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):*				
6.5.7 Cross-site scripting (XSS)	**6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)			
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	**6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)			
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)			

FTC-0002135

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows: ▪ Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: – At least annually – After any changes – By an organization that specializes in application security – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections ▪ Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. ***Note:*** *"An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*			

FTC-0002136

Copyright 2010 PCI Security Standards Council LLC

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following:			
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	**7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.			
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	**7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).			
7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	**7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges.			
7.1.4 Implementation of an automated access control system	**7.1.4** Confirm that access controls are implemented via an automated access control system.			
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:			
7.2.1 Coverage of all system components	**7.2.1** Confirm that access control systems are in place on all system components.			

FTC-0002137

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
7.2.2 Assignment of privileges to individuals based on job classification and function	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.			
7.2.3 Default "deny-all" setting ***Note:*** *Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.			

FTC-0002138

Copyright 2010 PCI Security Standards Council LLC

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Note: *These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data.			
8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: ▪ Something you know, such as a password or passphrase ▪ Something you have, such as a token device or smart card ▪ Something you are, such as a biometric	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following: ▪ Obtain and examine documentation describing the authentication method(s) used. ▪ For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).			

FTC-0002139

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) ***Note:*** *Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used.			
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	**8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage.			
	8.4.b For service providers only, observe password files to verify that customer passwords are encrypted.			
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**8.5.1** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following: ▪ Obtain and examine an authorization form for each ID. ▪ Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system.			

FTC-0002140

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.2 Verify user identity before performing password resets.	**8.5.2** Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.			
8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.			
8.5.4 Immediately revoke access for any terminated users.	**8.5.4** Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.			
8.5.5 Remove/disable inactive user accounts at least every 90 days.	**8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled.			
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	**8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor.			
	8.5.6.b Verify that vendor remote access accounts are monitored while being used.			
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies.			
8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	**8.5.8.a** For a sample of system components, examine user ID lists to verify the following: ▪ Generic user IDs and accounts are disabled or removed ▪ Shared user IDs for system administration activities and other critical functions do not exist ▪ Shared and generic user IDs are not used to administer any system components			
	8.5.8.b Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited.			
	8.5.8.c Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested.			

FTC-0002141

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
8.5.9 Change user passwords at least every 90 days.	**8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.			
	8.5.9.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non-consumer users are given guidance as to when, and under what circumstances, passwords must change.			
8.5.10 Require a minimum password length of at least seven characters.	**8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.			
	8.5.10.b For service providers only, review internal processes and customer/user documentation to verify that that non-consumer user passwords are required to meet minimum length requirements.			
8.5.11 Use passwords containing both numeric and alphabetic characters.	**8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters.			
	8.5.11.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters.			
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	**8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.			
	8.5.12.b For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.			FTC-0002142

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	8.5.13.b For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts.			
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	**8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.			
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.			
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	**8.5.16.a** Review database and application configuration settings and verify that all users are authenticated prior to access.			
	8.5.16.b Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).			
	8.5.16.c Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators.			
	8.5.16.d Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).			

FTC-0002143

Copyright 2010 PCI Security Standards Council LLC

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. ▪ Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. ▪ Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.			
9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	**9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.			
	9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.			
	9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.			
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks.			

FTC-0002144

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.			
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	**9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following: ▪ Granting new badges, ▪ Changing access requirements, and ▪ Revoking terminated onsite personnel and expired visitor badges			
	9.2.b Verify that access to the badge system is limited to authorized personnel.			
	9.2.c Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors.			
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	**9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data.			
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	**9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel.			
	9.3.2.b Verify that visitor badges expire.			
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.			

FTC-0002145

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.			
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months.			
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	**9.5.a** Observe the storage location's physical security to confirm that backup media storage is secure.			
	9.5.b Verify that the storage location security is reviewed at least annually.			
9.6 Physically secure all media.	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).			
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**9.7** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.			
9.7.1 Classify media so the sensitivity of the data can be determined.	**9.7.1** Verify that all media is classified so the sensitivity of the data can be determined.			
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.			
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization.			
9.9 Maintain strict control over the storage and accessibility of media.	**9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.			
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.			

FTC-0002146

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following:			
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	**9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.			
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents.			
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	**9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).			

FTC-0002147

Copyright 2010 PCI Security Standards Council LLC

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	**10.2.1** Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Verify actions taken by any individual with root or administrative privileges are logged.			
10.2.3 Access to all audit trails	**10.2.3** Verify access to all audit trails is logged.			
10.2.4 Invalid logical access attempts	**10.2.4** Verify invalid logical access attempts are logged.			
10.2 5 Use of identification and authentication mechanisms	**10.2.5** Verify use of identification and authentication mechanisms is logged.			
10.2.6 Initialization of the audit logs	**10.2.6** Verify initialization of audit logs is logged.			
10.2.7 Creation and deletion of system-level objects	**10.2.7** Verify creation and deletion of system level objects are logged.			
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following:			

FTC-0002148

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.			
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.			
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.			
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.			
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.			
10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.			
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	**10.4.a** Verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.			
	10.4.b Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented:			
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.			
	10.4.1.b Verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers.			
10.4.2 Time data is protected.	**10.4.2.a** Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.			
	10.4.2.b Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.			

FTC-0002149

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.4.3 Time settings are received from industry-accepted time sources.	**10.4.3** Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).			
10.5 Secure audit trails so they cannot be altered.	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			
10.5.1 Limit viewing of audit trails to those with a job-related need.	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files.			
10.5.2 Protect audit trail files from unauthorized modifications.	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.			
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	**10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.			
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	**10.5.5** Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.			

FTC-0002150

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.*	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.			
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components.			
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year.			
	10.7.b Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.			

FTC-0002151

Copyright 2010 PCI Security Standards Council LLC

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	**11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.			
	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: ▪ WLAN cards inserted into system components ▪ Portable wireless devices connected to system components (for example, by USB, etc.) ▪ Wireless devices attached to a network port or network device			
	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.			
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.			
	11.1.e Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.			

FTC-0002152

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	**11.2** Verify that internal and external vulnerability scans are performed as follows:			
11.2.1 Perform quarterly internal vulnerability scans.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.			
	11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.			
	11.2.1.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			

FTC-0002153

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.*	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.			
	11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).			
	11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC.			
11.2.3 Perform internal and external scans after any significant change. ***Note:*** *Scans conducted after changes may be performed by internal staff.*	**11.2.3.a** Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.			
	11.2.3.b Review scan reports and verify that the scan process includes rescans until: ▪ For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS, ▪ For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.			
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			

FTC-0002154

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	**11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.			
	11.3.b Verify that noted exploitable vulnerabilities were corrected and testing repeated.			
	11.3.c Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).			
11.3.1 Network-layer penetration tests	**11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems.			
11.3.2 Application-layer penetration tests	**11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.			
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.			
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.			
Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.c** Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.			

FTC-0002155

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	**11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: ▪ System executables ▪ Application executables ▪ Configuration and parameter files ▪ Centrally stored, historical or archived, log and audit files			
	11.5.b Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.			

FTC-0002156

Copyright 2010 PCI Security Standards Council LLC

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).			
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.			
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.			
12.1.3 Includes a review at least annually and updates when the environment changes.	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	**12.2** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.			

FTC-0002157

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	**12.3** Obtain and examine the usage policies for critical technologies and perform the following:			
12.3.1 Explicit approval by authorized parties	**12.3.1** Verify that the usage policies require explicit approval from authorized parties to use the technologies.			
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).			
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices.			
12.3.4 Labeling of devices to determine owner, contact information and purpose	**12.3.4** Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose.			
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology.			
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology.			
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products.			
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.			
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.			

FTC-0002158

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.			
	12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**12.4** Verify that information security policies clearly define information security responsibilities for all personnel.			
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures.	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned.			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.			
12.5.4 Administer user accounts, including additions, deletions, and modifications	**12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned.			
12.5.5 Monitor and control all access to data.	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned.			

FTC-0002159

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	**12.6.a** Verify the existence of a formal security awareness program for all personnel.			
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).			
	12.6.1.b Verify that personnel attend awareness training upon hire and at least annually.			
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.			
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	**12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.			
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	**12.8** If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following:			
12.8.1 Maintain a list of service providers.	**12.8.1** Verify that a list of service providers is maintained.			

FTC-0002160

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	**12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data.			
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**12.8.3** Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.			
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.			
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises ▪ Coverage and responses of all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands	**12.9.1.a** Verify that the incident response plan includes: ▪ Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum: ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) ▪ Coverage and responses for all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands			
	12.9.1.b Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed.			

FTC-0002161

Copyright 2010 PCI Security Standards Council LLC

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.9.2 Test the plan at least annually.	**12.9.2** Verify that the plan is tested at least annually.			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**12.9.3** Verify through observation and review of policies, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.			
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	**12.9.4** Verify through observation and review of policies that staff with responsibilities for security breach response are periodically trained.			
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.			
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.			

FTC-0002162

Copyright 2010 PCI Security Standards Council LLC

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below:			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: No entity on the system can use a shared web server user ID. All CGI scripts used by an entity must be created and run as the entity's unique user ID.			

FTC-0002163

Copyright 2010 PCI Security Standards Council LLC

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).			
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.) **Important:** An entity's files may not be shared by group.			
	A.1.2.c Verify that an entity's users do not have write access to shared system binaries.			
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity.			
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: ▪ Disk space ▪ Bandwidth ▪ Memory ▪ CPU			
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	**A.1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: Logs are enabled for common third-party applications. Logs are active by default. Logs are available for review by the owning entity. Log locations are clearly communicated to the owning entity.			
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.			

FTC-0002164

Copyright 2010 PCI Security Standards Council LLC

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

Note: *The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if: (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

FTC-0002165

Copyright 2010 PCI Security Standards Council LLC

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	

FTC-0002166

Copyright 2010 PCI Security Standards Council LLC

Compensating Controls Worksheet – Completed Example

Use this worksheet to define compensating controls for any requirement noted as "in place" via compensating controls.

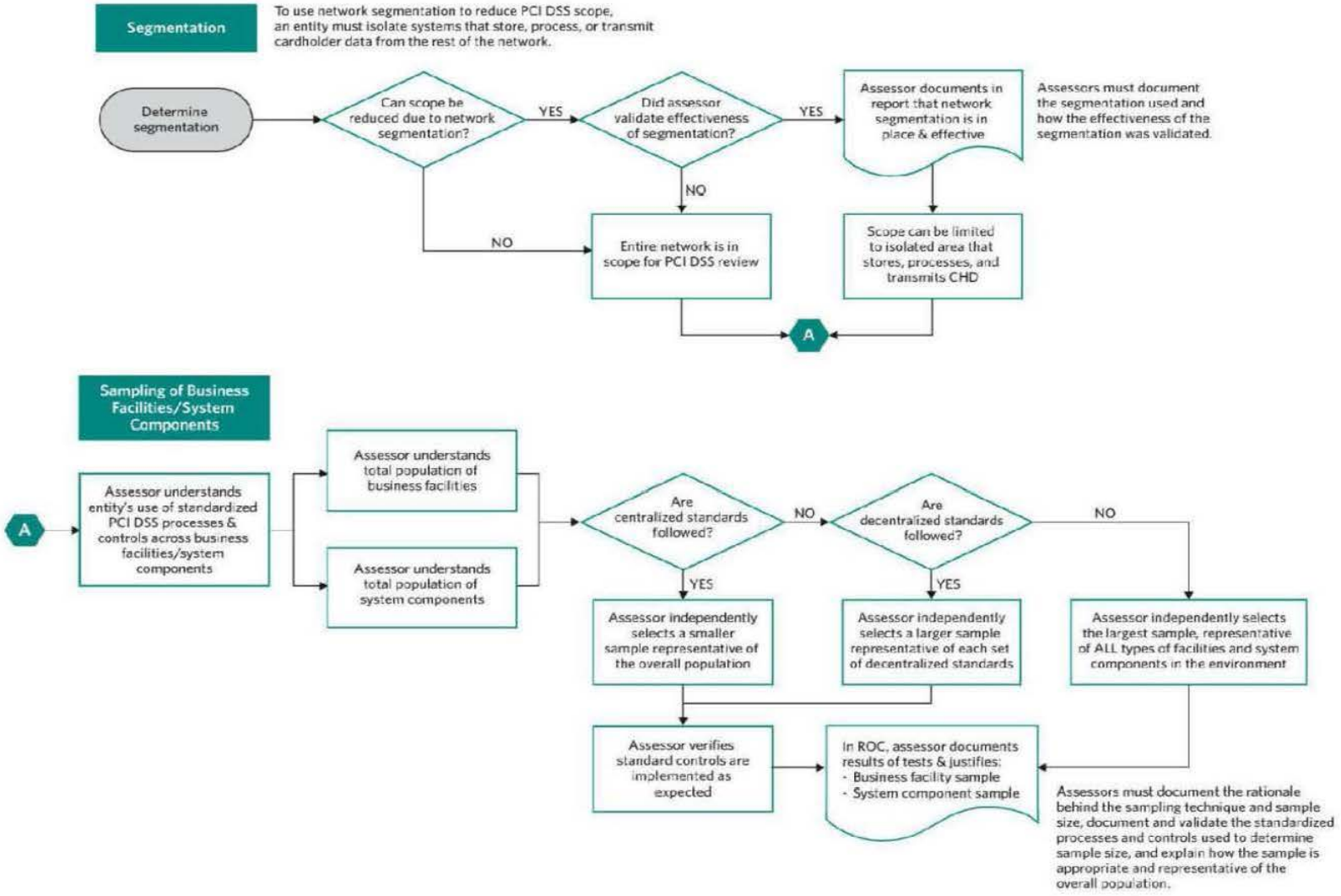
Requirement Number: *8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the SU-log directory. In this way, each user's actions can be tracked through the SU account.*
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges.*
6. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged.*

FTC-0002167

Copyright 2010 PCI Security Standards Council LLC

Appendix D: Segmentation and Sampling of Business Facilities/System Components



FTC-0002168

Copyright 2010 PCI Security Standards Council LLC

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 8
TO EXPERT REPORT OF DR. ERIC B. COLE

NIST Special Publication 800-53A
Revision 1

National Institute of Standards and Technology
U.S. Department of Commerce

Guide for Assessing the Security Controls in Federal Information Systems and Organizations

Building Effective Security Assessment Plans

JOINT TASK FORCE TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Consistent with NIST SP 800-53, Revision 3

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Special Publication 800-53A, Revision 1, 399 pages

(June 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

In accordance with the provisions of FISMA,[1] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

- Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.[2] FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.
- Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.[3]
- Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.
- Compliance schedules for NIST security standards and guidelines are established by OMB in policies, directives, or memoranda (e.g., annual FISMA Reporting Guidance).[4]

---

[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. Given the high priority of information sharing and transparency within the federal government, agencies also consider reciprocity in developing their information security solutions. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

[4] Unless otherwise stated, all references to NIST publications in this document (i.e., Federal Information Processing Standards and Special Publications) are to the most recent version of the publication.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency technical working group whose dedicated efforts contributed significantly to the publication. The senior leaders, interagency working group members, and their organizational affiliations include:

U.S. Department of Defense

Cheryl J. Roby
Acting Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer

Gus Guissanie
Acting Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance

Dominic Cussatt
Senior Policy Advisor

Office of the Director of National Intelligence

Honorable Priscilla Guthrie
Intelligence Community Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief Information Officer

Mark J. Morrison
Deputy Associate Director of National Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Cyber Security Advisor, Information Technology Laboratory

Donna Dodson
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Dave Wennergren
Acting Chair, CNSS

Eustace D. King
CNSS Subcommittee Co-Chair (DoD)

Peter Gouldmann
CNSS Subcommittee Co-Chair (DoS)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross
NIST, JTF Leader

Patricia Toth
NIST

Bennett Hodge
Booz Allen Hamilton

Gary Stoneburner
Johns Hopkins APL

Esten Porter
The MITRE Corporation

Karen Quigg
The MITRE Corporation

Terry Sherald
Department of Defense

Peter Gouldmann
Department of State

Jonathan Chiu
Booz Allen Hamilton

Kelley Dempsey
NIST

Arnold Johnson
NIST

Christian Enloe
NIST

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon of NIST for their superb technical editing and administrative support. The authors also wish to recognize Jennifer Fabius Greene, James Govekar, Terrance Hazelwood, Austin Hershey, Laurie Hestor, Jason Mackanick, Timothy Potter, Jennifer Puma, Matthew Scholl, Julie Trei, Gail Tryon, Ricki Vanetesse, Cynthia Whitmer, and Peter Williams for their exceptional contributions in helping to improve the content of the publication. And finally, the authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality and usefulness of this publication.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by FISMA, NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. A common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Table of Contents

CHAPTER ONE INTRODUCTION 1
1.1 PURPOSE AND APPLICABILITY 1
1.2 TARGET AUDIENCE 3
1.3 RELATED PUBLICATIONS AND ASSESSMENT PROCESSES 4
1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION 5
CHAPTER TWO THE FUNDAMENTALS 6
2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE 6
2.2 STRATEGY FOR CONDUCTING SECURITY CONTROL ASSESSMENTS 7
2.3 BUILDING AN EFFECTIVE ASSURANCE CASE 8
2.4 ASSESSMENT PROCEDURES 9
CHAPTER THREE THE PROCESS 13
3.1 PREPARING FOR SECURITY CONTROL ASSESSMENTS 13
3.2 DEVELOPING SECURITY ASSESSMENT PLANS 15
3.3 CONDUCTING SECURITY CONTROL ASSESSMENTS 22
3.4 ANALYZING SECURITY ASSESSMENT REPORT RESULTS 24
APPENDIX A REFERENCES A-1
APPENDIX B GLOSSARY B-1
APPENDIX C ACRONYMS C-1
APPENDIX D ASSESSMENT METHOD DESCRIPTIONS D-1
APPENDIX E PENETRATION TESTING E-1
APPENDIX F ASSESSMENT PROCEDURE CATALOG F-1
APPENDIX G SECURITY ASSESSMENT REPORTS G-1
APPENDIX H ASSESSMENT CASES H-1

FTC-0002349

Prologue

"…Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations…"

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

Preface

Security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits—rather, security controls assessments are the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, is written to facilitate security control assessments conducted within an effective risk management framework. The assessment results provide organizational officials with:

- Evidence about the effectiveness of security controls in organizational information systems;
- An indication of the quality of the risk management processes employed within the organization; and
- Information about the strengths and weaknesses of information systems which are supporting organizational missions and business functions in a global environment of sophisticated and changing threats.

The findings produced by assessors are used to determine the overall effectiveness of the security controls associated with an information system (including system-specific, common, and hybrid controls) and to provide credible and meaningful inputs to the organization's risk management process. A well-executed assessment helps to: (i) determine the validity of the security controls contained in the security plan and subsequently employed in the information system and its environment of operation; and (ii) facilitate a cost-effective approach to correcting weaknesses or deficiencies in the system in an orderly and disciplined manner consistent with organizational mission/business needs.

Special Publication 800-53A is a companion guideline to Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. Each publication provides guidance for implementing specific steps in the Risk Management Framework (RMF).[5] Special Publication 800-53 covers Step 2 in the RMF, security control selection (i.e., determining what security controls are needed to manage risks to organizational operations and assets, individuals, other organizations, and the Nation). Special Publication 800-53A covers RMF Step 4, security control assessment, and RMF Step 6, continuous monitoring, and provides guidance on the security assessment process. This guidance includes how to build effective security assessment plans and how to analyze and manage assessment results.

Special Publication 800-53A allows organizations to tailor and supplement the basic assessment procedures provided. The concepts of tailoring and supplementation used in this document are similar to the concepts described in Special Publication 800-53. Tailoring involves scoping the assessment procedures to more closely match the characteristics of the information system and its environment of operation. The tailoring process gives organizations the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements established by applying the fundamental concepts in the RMF. Supplementation involves adding assessment procedures or assessment details to adequately meet the risk management needs of the organization (e.g., adding organization-specific details such as system/platform-specific information for selected security controls). Supplementation decisions are left to the discretion of the organization in order to maximize

[5] Special Publication 800-37 provides guidance on applying the RMF to federal information systems.

FTC-0002351

flexibility in developing security assessment plans when applying the results of risk assessments in determining the extent, rigor, and level of intensity of the assessments.

While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration. A major design objective for Special Publication 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are essential for achieving such consistency. In addition to the assessment framework and initial starting point for assessment procedures, NIST initiated an *Assessment Case Development Project*.[6] The purpose of the project is fourfold: (i) to actively engage experienced assessors from multiple organizations in the development of a representative set of assessment cases corresponding to the assessment procedures in Special Publication 800-53A; (ii) to provide organizations and the assessors supporting those organizations with an exemplary set of assessment cases for each assessment procedure in the catalog of procedures in this publication; (iii) to provide a vehicle for ongoing community-wide review of the assessment cases to promote continuous improvement in the assessment process for more consistent, cost-effective security assessments of federal information systems; and (iv) to serve as a basis for reciprocity among various communities of interest. The Assessment Case Development Project is described in Appendix H.

In addition to the assessment case project supporting this publication, NIST also initiated the Security Content Automation Protocol (SCAP)[7] project that supports and complements the approach for achieving consistent, cost-effective security control assessments. The primary purpose of the SCAP is to improve the automated application, verification, and reporting of information technology product-specific security configuration settings, enabling organizations to identify and reduce the vulnerabilities associated with products that are not configured properly. As part of this initiative, an Open Checklist Interactive Language (OCIL)[8] provides the capability to express the determination statements in the assessment procedures in Appendix F in a framework that will establish interoperability with the validated tool sets supporting SCAP.

[6] An *assessment case* represents a worked example of an assessment procedure that provides specific actions that an assessor might carry out during the assessment of a security control or control enhancement in an information system.

[7] Special Publication 800-126 provides guidance on the technical specification of the SCAP. Additional details on the SCAP initiative, as well as freely available SCAP reference data, can be found at http://nvd.nist.gov.

[8] OCIL is a framework for expressing security checks that cannot be evaluated without some human interaction or feedback. It is used to determine the state of a system by presenting one or more questionnaires to its intended users. The language includes constructs for questions, instructions for guiding users towards an answer, responses to questions, artifacts, and evaluation results.

CAUTIONARY NOTES

Organizations should carefully consider the potential impacts of employing the assessment procedures defined in this Special Publication when assessing the security controls in *operational* information systems. Certain assessment procedures, particularly those procedures that directly impact the operation of hardware, software, or firmware components of an information system, may inadvertently affect the routine processing, transmission, or storage of information supporting organizational missions or business functions. For example, a critical information system component may be taken offline for assessment purposes or a component may suffer a fault or failure during the assessment process. Organizations should also take necessary precautions during security assessment periods to ensure that organizational missions and business functions continue to be supported by the information system and that any potential impacts to operational effectiveness resulting from the assessment are considered in advance.

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS SECURITY CONTROL EFFECTIVENESS IN INFORMATION SYSTEMS

Today's information systems[9] are complex assemblages of technology (i.e., hardware, software, and firmware), processes, and people, working together to provide organizations with the capability to process, store, and transmit information in a timely manner to support various missions and business functions. The degree to which organizations have come to depend upon these information systems to conduct routine, important, and critical missions and business functions means that the protection of the underlying systems is paramount to the success of the organization. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization as well as the welfare of individuals.[10] Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information. Once employed within an information system, security controls are assessed to provide the information necessary to determine their overall effectiveness; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system and its environment of operation is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the Nation resulting from the use of the system.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. The guidelines apply to the security controls defined in Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems and Organizations*. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Enabling more consistent, comparable, and repeatable assessments of security controls with reproducible results;
- Facilitating more cost-effective assessments of security controls contributing to the determination of overall control effectiveness;
- Promoting a better understanding of the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems; and

[9] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[10] When selecting security controls for an information system, the organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts.

- Creating more complete, reliable, and trustworthy information for organizational officials to support risk management decisions, reciprocity of assessment results, information sharing, and FISMA compliance.

This publication satisfies the requirements of the Federal Information Security Management Act (FISMA) and meets or exceeds the information security requirements established for executive agencies[11] by the Office of Management and Budget (OMB) in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*. The guidelines in this publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems. State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.[12]

Organizations use this publication in conjunction with an approved security plan in developing a viable security assessment plan for producing and compiling the information necessary to determine the effectiveness of the security controls employed in the information system. This publication has been developed with the intention of enabling organizations to tailor and supplement the basic assessment procedures provided. The assessment procedures are used as a starting point for and as input to the security assessment plan. In developing effective security assessment plans, organizations take into consideration existing information about the security controls to be assessed (e.g., results from organizational assessments of risk, platform-specific dependencies in the hardware, software, or firmware, and any assessment procedures needed as a result of organization-specific controls not included in Special Publication 800-53).[13]

The selection of appropriate assessment procedures and the rigor, intensity, and scope of the assessment depend on three factors:

- The security categorization of the information system;[14]
- The assurance requirements that the organization intends to meet in determining the overall effectiveness of the security controls; and

[11] An *executive agency* is: (i) an executive department specified in 5 U.S.C., Section 101; (ii) a military department specified in 5 U.S.C., Section 102; (iii) an independent establishment as defined in 5 U.S.C., Section 104(1); and (iv) a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. In this publication, the term executive agency is synonymous with the term *federal agency*.

[12] In accordance with the provisions of FISMA and OMB policy, whenever the interconnection of federal information systems to information systems operated by state/local/tribal governments, contractors, or grantees involves the processing, storage, or transmission of federal information, the information security standards and guidelines described in this publication apply. Specific information security requirements and the terms and conditions of the system interconnections, are expressed in the Memorandums of Understanding and Interconnection Security Agreements established by participating organizations.

[13] For example, detailed test scripts may need to be developed for the specific operating system, network component, middleware, or application employed within the information system to adequately assess certain characteristics of a particular security control. Such test scripts are at a lower level of detail than provided by the assessment procedures contained in Appendix F (Assessment Procedures Catalog) and are therefore beyond the scope of this publication. Additional details for assessments are provided in the supporting assessment cases described in Appendix H.

[14] For national security systems, security categorization is accomplished in accordance with CNSS Instruction 1253. For other than national security systems, security categorization is accomplished in accordance with FIPS 199 and Special Publication 800-60.

- The selection of security controls from Special Publication 800-53 as identified in the approved security plan.[15]

The assessment process is an information-gathering activity, not a security-producing activity. Organizations determine the most cost-effective implementation of this key element in the organization's information security program by applying the results of risk assessments, considering the maturity and quality level of the organization's risk management processes, and taking advantage of the flexibility in the concepts described in this publication. The use of Special Publication 800-53A as a starting point in the process of defining procedures for assessing the security controls in information systems and organizations, promotes a consistent level of security and offers the needed flexibility to customize the assessment based on organizational policies and requirements, known threat and vulnerability information, operational considerations, information system and platform dependencies, and tolerance for risk.[16] The information produced during security control assessments can be used by an organization to:

- Identify potential problems or shortfalls in the organization's implementation of the Risk Management Framework;
- Identify information system weaknesses and deficiencies;
- Prioritize risk mitigation decisions and associated risk mitigation activities;
- Confirm that identified weaknesses and deficiencies in the information system have been addressed;
- Support continuous monitoring activities and information security situational awareness;
- Facilitate security authorization decisions; and
- Inform budgetary decisions and the capital investment process.

Organizations are not expected to employ *all* of the assessment methods and assessment objects contained within the assessment procedures identified in this publication for the associated security controls deployed within or inherited by organizational information systems. Rather, organizations have the inherent flexibility to determine the level of effort needed for a particular assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made on the basis of what will accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the subsequent determination of the resulting mission or business risk.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of information system and information security professionals including:

- Individuals with information system development and integration responsibilities (e.g., program managers, information technology product developers, information system developers, systems integrators, information security architects);

[15] The security controls for the information system are documented in the security plan after the initial selection, tailoring, and supplementation of the controls as described in NIST Special Publication 800-53 and CNSS Instruction 1253. The security plan is approved by the authorizing official with recommendations from other appropriate organizational officials prior to the start of the security control assessment.

[16] In this publication, the term *risk* is used to mean risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

- Individuals with information security assessment and continuous monitoring responsibilities (e.g., system evaluators/testers, penetration testers, security control assessors, independent verifiers and validators, auditors, information system owners, common control providers);
- Individuals with information system and security management and oversight responsibilities (e.g., authorizing officials, senior information security officers,[17] information security managers); and
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, common control providers, information owners/stewards, mission owners, systems administrators, information system security officers).

1.3 RELATED PUBLICATIONS AND ASSESSMENT PROCESSES

Special Publication 800-53A is designed to support Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. In particular, the assessment procedures contained in this publication and the guidelines provided for developing security assessment plans for organizational information systems directly support the security control assessment and continuous monitoring activities that are integral to the risk management process. This includes providing near real-time information to organizational officials regarding the ongoing security state of their information systems.

Organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available on information system components from previous assessments including independent third-party testing, evaluation, and validation.[18] Product testing, evaluation, and validation may be conducted on cryptographic modules and general-purpose information technology products such as operating systems, database systems, firewalls, intrusion detection devices, Web browsers, Web applications, smart cards, biometrics devices, personal identity verification devices, network devices, and hardware platforms using national and international standards. If an information system component product is identified as providing support for the implementation of a particular security control in Special Publication 800-53, then evidence produced during the product testing, evaluation, and validation processes (e.g., security specifications, analyses and test results, validation reports, and validation certificates)[19] is used to the extent that it is applicable. This evidence is combined with the assessment-related evidence obtained from the application of the assessment procedures in this publication, to cost-effectively produce the information necessary to determine whether the security controls are effective in their application.

---

[17] At the *agency* level, this position is known as the Senior Agency Information Security Officer. Organizations may also refer to this position as the *Chief Information Security Officer*.

[18] Assessment results can be obtained from many activities that occur routinely during the system development life cycle. For example, assessment results are produced during the testing and evaluation of new information system components during system upgrades or system integration activities. Organizations can take advantage of previous assessment results whenever possible, to reduce the overall cost of assessments and to make the assessment process more efficient.

[19] Organizations review the available information from component information technology products to determine: (i) what security controls are implemented by the product; (ii) if those security controls meet the intended control requirements of the information system under assessment; (iii) if the configuration of the product and the environment in which the product operates are consistent with the environmental and product configuration stated by the vendor and/or developer; and (iv) if the assurance requirements stated in the developer/vendor specification satisfy the assurance requirements for assessing those controls. Meeting the above criteria provides a sound rationale that the product is suitable and meets the intended security control requirements of the information system under assessment.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control assessments including: (i) the integration of assessments into the system development life cycle; (ii) the importance of an organization-wide strategy for conducting security control assessments; (iii) the development of effective assurance cases to help increase the grounds for confidence in the effectiveness of the security controls being assessed; and (iv) the format and content of assessment procedures.
- **Chapter Three** describes the process of assessing the security controls in organizational information systems and their environments of operation including: (i) the activities carried out by organizations and assessors to prepare for security control assessments; (ii) the development of security assessment plans; (iii) the conduct of security control assessments and the analysis, documentation, and reporting of assessment results; and (iv) the post-assessment report analysis and follow-on activities carried out by organizations.
- **Supporting appendices** provide detailed assessment-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) a description of assessment methods; (v) penetration testing guidelines; (vi) a master catalog of assessment procedures that can be used to develop plans for assessing security controls; (vii) content of security assessment reports; and (viii) the definition, format, and use of assessment cases.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH SECURITY CONTROL ASSESSMENTS

This chapter describes the basic concepts associated with assessing the security controls in organizational information systems including: (i) the integration of assessments into the system development life cycle; (ii) the importance of an organization-wide strategy for conducting security control assessments; (iii) the development of effective assurance cases to help increase the grounds for confidence in the effectiveness of the security controls; and (iv) the format and content of assessment procedures.

2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE

Security assessments can be effectively carried out at various stages in the system development life cycle[20] to increase the grounds for confidence that the security controls employed within or inherited by an information system are effective in their application. This publication provides a comprehensive set of assessment procedures to support security assessment activities throughout the system development life cycle. For example, security assessments are routinely conducted by information system developers and system integrators during the development/acquisition and implementation phases of the life cycle to help ensure that the required security controls for the system are properly designed and developed, correctly implemented, and consistent with the established organizational information security architecture. Assessment activities in the initial system development life cycle phases include, for example, design and code reviews, application scanning, and regression testing. Security weaknesses and deficiencies identified early in the system development life cycle can be resolved more quickly and in a much more cost-effective manner before proceeding to subsequent phases in the life cycle. The objective is to identify the information security architecture and security controls up front and to ensure that the system design and testing validate the implementation of these controls. The assessment procedures described in Appendix F can support these types of assessments carried out during the initial stages of the system development life cycle.

Security assessments are also routinely conducted by information system owners, common control providers, information system security officers, independent assessors, auditors, and Inspectors General during the operations and maintenance phase of the life cycle to ensure that security controls are effective and continue to be effective in the operational environment where the system is deployed. For example, organizations assess all security controls employed within and inherited by the information system during the initial security authorization. Subsequent to the initial authorization, the organization assesses the security controls (including management, operational, and technical controls) on an ongoing basis. The frequency of such monitoring is based on the continuous monitoring strategy developed by the information system owner or common control provider and approved by the authorizing official.[21] Finally, at the end of the life cycle, security assessments are conducted as part of ensuring that important organizational information is purged from the information system prior to disposal.

[20] There are typically five phases in a generic system development life cycle: (i) initiation; (ii) development/acquisition; (iii) implementation; (iv) operations and maintenance; and (v) disposition (disposal).

[21] Special Publication 800-37 provides guidance on the continuous monitoring of security controls.

2.2 STRATEGY FOR CONDUCTING SECURITY CONTROL ASSESSMENTS

Organizations are encouraged to develop a broad-based, organization-wide strategy for conducting security assessments, facilitating more cost-effective and consistent assessments across the inventory of information systems. An organization-wide strategy begins by applying the initial steps of the Risk Management Framework to all information systems within the organization, with an organizational view of the security categorization process and the security control selection process (including the identification of common controls). Categorizing information systems as an organization-wide activity taking into consideration the enterprise architecture and the information security architecture helps to ensure that the individual systems are categorized based on the mission and business objectives of the organization. Maximizing the number of common controls employed within an organization: (i) significantly reduces the cost of development, implementation, and assessment of security controls; (ii) allows organizations to centralize security control assessments and to amortize the cost of those assessments across all information systems organization-wide; and (iii) increases overall security control consistency. An organization-wide approach to identifying common controls early in the application of the RMF facilitates a more global strategy for assessing those controls and sharing essential assessment results with information system owners and authorizing officials. The sharing of assessment results among key organizational officials across information system boundaries has many important benefits including:

- Providing the capability to review assessment results for all information systems and to make organization-wide, mission/business-related decisions on risk mitigation activities according to organizational priorities, the security categorization of the information systems supporting the organization, and risk assessments;
- Providing a more global view of systemic weaknesses and deficiencies occurring in information systems across the organization;
- Providing an opportunity to develop organization-wide solutions to information security problems; and
- Increasing the organization's knowledge base regarding threats, vulnerabilities, and strategies for more cost-effective solutions to common information security problems.

Organizations can also promote a more focused and cost-effective assessment process by: (i) developing more specific assessment procedures that are tailored for their specific organizational environments of operation and requirements (instead of relegating these tasks to each security control assessor or assessment team); and (ii) providing organization-wide tools, templates, and techniques to support more consistent assessments throughout the organization.

While the conduct of security control assessments is the primary responsibility of information system owners and common control providers with oversight by their respective authorizing officials, there is also significant involvement in the assessment process by other parties within the organization who have a vested interest in the outcome of assessments. Other interested parties include, for example, mission/business owners, information owners/stewards (when those roles are filled by someone other than the information system owner), information security officials, and the risk executive (function). It is imperative that information system owners and common control providers coordinate with the other parties in the organization having an interest in security control assessments to help ensure that the organization's core missions and business functions are adequately addressed in the selection of security controls to be assessed.

2.3 BUILDING AN EFFECTIVE ASSURANCE CASE

Building an effective assurance case[22] for security control effectiveness is a process that involves: (i) compiling evidence from a variety of activities conducted during the system development life cycle that the controls employed in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system; and (ii) presenting this evidence in a manner that decision makers are able to use effectively in making risk-based decisions about the operation or use of the system. The evidence described above comes from the implementation of the security controls in the information system and inherited by the system (i.e., common controls) and from the assessments of that implementation. Ideally, the assessor is building on previously developed materials that started with the specification of the organization's information security needs and was further developed during the design, development, and implementation of the information system. These materials, developed while implementing security throughout the life cycle of the information system, provide the initial evidence for an assurance case.

Assessors obtain the required evidence during the assessment process to allow the appropriate organizational officials to make objective determinations about the effectiveness of the security controls and the overall security state of the information system. The assessment evidence needed to make such determinations can be obtained from a variety of sources including, but not limited to, information technology product and system assessments. Product assessments (also known as product testing, evaluation, and validation) are typically conducted by independent, third-party testing organizations. These assessments examine the security functions of products and established configuration settings. Assessments can be conducted against industry, national, or international information security standards as well as developer/vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in millions of information systems, these types of assessments can be carried out at a greater level of depth and provide deeper insights into the security capabilities of the particular products.

System assessments are typically conducted by information systems developers, systems integrators, information system owners, common control providers, assessors, auditors, Inspectors General, and the information security staffs of organizations. The assessors or assessment teams bring together available information about the information system such as the results from individual component product assessments, if available, and conduct additional system-level assessments using a variety of methods and techniques. System assessments are used to compile and evaluate the evidence needed by organizational officials to determine how effective the security controls employed in the information system are likely to be in mitigating risks to organizational operations and assets, to individuals, to other organizations, and to the Nation. The results from assessments conducted using information system-specific and organization-specific assessment procedures derived from the guidelines in this publication contribute to compiling the necessary evidence to determine security control effectiveness in accordance with the assurance requirements documented in the security plan.

[22] An assurance case is a body of evidence organized into an argument demonstrating that some claim about an information system holds (i.e., is assured). An assurance case is needed when it is important to show that a system exhibits some complex property such as safety, security, or reliability. Additional information can be obtained at https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/assurance/643.html.

2.4 ASSESSMENT PROCEDURES

An assessment procedure consists of a set of assessment *objectives*, each with an associated set of potential assessment *methods* and assessment *objects*. An assessment objective includes a set of *determination statements* related to the security control under assessment. The determination statements are linked to the content of the security control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements. The application of an assessment procedure to a security control produces assessment *findings*. These assessment findings reflect, or are subsequently used, to help determine the overall effectiveness of the security control.

Assessment objects identify the specific items being assessed and include *specifications*, *mechanisms*, *activities*, and *individuals*. Specifications are the document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. Mechanisms are the specific hardware, software, or firmware safeguards and countermeasures employed within an information system.[23] Activities are the specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising a contingency plan). Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.

Assessment methods define the nature of the assessor actions and include *examine*, *interview*, and *test*. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence. The *interview* method is the process of holding discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence. The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior. In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure. A complete description of assessment methods and assessment objects is provided in Appendix D.

The assessment methods have a set of associated attributes, *depth* and *coverage*, which help define the level of effort for the assessment. These attributes are hierarchical in nature, providing the means to define the rigor and scope of the assessment for the increased assurances that may be needed for some information systems. The depth attribute addresses the rigor of and level of detail in the examination, interview, and testing processes. Values for the depth attribute include *basic*, *focused*, and *comprehensive*. The coverage attribute addresses the scope or breadth of the examination, interview, and testing processes including the number and type of specifications, mechanisms, and activities to be examined or tested and the number and types of individuals to be interviewed. Similar to the depth attribute, values for the coverage attribute include *basic*, *focused*, and *comprehensive*. The appropriate depth and coverage attribute values for a particular assessment method are based on the assurance requirements specified by the organization.[24] As assurance requirements increase with regard to the development, implementation, and operation

[23] Mechanisms also include physical protection devices associated with an information system (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes, etc.).

[24] For other than national security systems, organizations meet minimum assurance requirements specified in Special Publication 800-53, Appendix E.

of security controls within or inherited by the information system, the rigor and scope of the assessment activities (as reflected in the selection of assessment methods and objects and the assignment of depth and coverage attribute values), tend to increase as well. Appendix D provides a detailed description of assessment method attributes and attribute values.

While flexibility continues to be an important factor in developing security assessment plans, consistency of assessments is also an important consideration. A major design objective for Special Publication 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are essential for achieving such consistency. In addition to the assessment framework and initial starting point for assessment procedures, Appendix H describes the Assessment Case Development Project. The purpose of this project is fourfold: (i) to actively engage experienced assessors in the development of a representative set of assessment cases corresponding to the assessment procedures in Appendix F; (ii) to provide organizations and the assessors supporting those organizations with an exemplary set of assessment cases for each assessment procedure in the catalog of procedures in Appendix F; (iii) to provide a vehicle for ongoing community-wide review of the assessment cases to promote continuous improvement in the assessment process for more consistent, cost-effective security assessments of federal information systems; and (iv) to serve as a basis of reciprocity among various communities of interest. Appendix H contains several examples of assessment cases.

AN EXAMPLE ASSESSMENT PROCEDURE

SECURITY CONTROL	
CP-2	**CONTINGENCY PLAN**
Control:	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

SECURITY CONTROL	
CP-2	**CONTINGENCY PLAN**
Supplemental Guidance:	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.

The first assessment objective for CP-2 is derived from the basic control statement. Potential assessment methods and objects are added to the assessment procedure.

ASSESSMENT PROCEDURE	
CP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a contingency plan for the information system that:* - *identifies essential missions and business functions and associated contingency requirements;* - *provides recovery objectives, restoration priorities, and metrics;* - *addresses contingency roles, responsibilities, assigned individuals with contact information;* - *addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and* - *addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and* - *is reviewed and approved by designated officials within the organization;* *(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan; and* *(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records].[25] **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

[25] Although not explicitly noted with each identified assessment method in the assessment procedure format in Appendix F, the attribute values of *depth* and *coverage* described in Appendix D are assigned by the organization and applied by the assessor/assessment team in the execution of the assessment method against an assessment object.

In a similar manner, the second assessment objective and potential assessment methods and objects for CP-2 are established.

ASSESSMENT PROCEDURE	
CP-2.2	*Determine if:* *(i) the organization coordinates contingency planning activities with incident handling activities;* *(ii) the organization defines the frequency of contingency plan reviews;* *(iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;* *(iv) the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing; and* *(v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements as identified in CP-2.1 (ii).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities].

The assessment objectives within a particular assessment procedure are numbered sequentially (e.g., CP-2.1,…, CP-2.n). If the security control has any enhancements, assessment objectives are developed for each enhancement using the same process as for the base control. The resulting assessment objectives within the assessment procedure are numbered sequentially (e.g., CP-2(1).1 indicating the first assessment objective for the first enhancement for security control CP-2).

CHAPTER THREE

THE PROCESS

CONDUCTING EFFECTIVE SECURITY CONTROL ASSESSMENTS

This chapter describes the process of assessing the security controls in organizational information systems including: (i) the activities carried out by organizations and assessors to prepare for security control assessments; (ii) the development of security assessment plans; (iii) the conduct of security control assessments and the analysis, documentation, and reporting of assessment results; and (iv) post-assessment report analysis and follow-on activities carried out by organizations.

3.1 PREPARING FOR SECURITY CONTROL ASSESSMENTS

Conducting security control assessments in today's complex environment of sophisticated information technology infrastructures and high-visibility, mission-critical applications can be difficult, challenging, and resource-intensive. Success requires the cooperation and collaboration among all parties having a vested interest in the organization's information security posture, including information system owners, common control providers, authorizing officials, chief information officers, senior information security officers, chief executive officers/heads of agencies, Inspectors General, and the OMB. Establishing an appropriate set of expectations before, during, and after the assessment is paramount to achieving an acceptable outcome—that is, producing information necessary to help the authorizing official make a credible, risk-based decision on whether to place the information system into operation or continue its operation.

Thorough preparation by the organization and the assessors is an important aspect of conducting effective security control assessments. Preparatory activities address a range of issues relating to the cost, schedule, and performance of the assessment. From the organizational perspective, preparing for a security control assessment includes the following key activities:

- Ensuring that appropriate policies covering security control assessments are in place and understood by all affected organizational elements;
- Ensuring that all steps in the RMF prior to the security control assessment step, have been successfully completed and received appropriate management oversight;[26]
- Ensuring that security controls identified as common controls (and the common portion of hybrid controls) have been assigned to appropriate organizational entities (i.e., common control providers) for development and implementation;[27]
- Establishing the objective and scope of the security control assessment (i.e., the purpose of the assessment and what is being assessed);

[26] Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments.

[27] Security control assessments include common controls that are the responsibility of organizational entities other than the information system owner inheriting the controls or hybrid controls where there is shared responsibility among the system owner and designated organizational entities.

- Notifying key organizational officials of the impending security control assessment and allocating necessary resources to carry out the assessment;
- Establishing appropriate communication channels among organizational officials having an interest in the security control assessment;[28]
- Establishing time frames for completing the security control assessment and key milestone decision points required by the organization to effectively manage the assessment;
- Identifying and selecting a competent assessor/assessment team that will be responsible for conducting the security control assessment, considering issues of assessor independence;
- Collecting artifacts to provide to the assessor/assessment team (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous assessment results); and
- Establishing a mechanism between the organization and the assessor and/or assessment team to minimize ambiguities or misunderstandings about security control implementation or security control weaknesses/deficiencies identified during the assessment.

Security control assessors/assessment teams begin preparing for the assessment by:

- Obtaining a general understanding of the organization's operations (including mission, functions, and business processes) and how the information system that is the subject of the security control assessment supports those organizational operations;
- Obtaining an understanding of the structure of the information system (i.e., system architecture);
- Obtaining a thorough understanding of the security controls being assessed (including system-specific, hybrid, and common controls);
- Identifying the organizational entities responsible for the development and implementation of the common controls (or the common portion of hybrid controls) supporting the information system;
- Establishing appropriate organizational points of contact needed to carry out the security control assessment;
- Obtaining artifacts needed for the security control assessment (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous assessment results);
- Obtaining previous assessment results that may be appropriately reused for the security control assessment (e.g., Inspector General reports, audits, vulnerability scans, physical security inspections, prior assessments, developmental testing and evaluation, vendor flaw remediation activities , ISO/IEC 15408 [Common Criteria] evaluations);
- Meeting with appropriate organizational officials to ensure common understanding for assessment objectives and the proposed rigor and scope of the assessment; and
- Developing a security assessment plan.

[28] Typically, these individuals include authorizing officials, information system owners, common control providers, mission and information owners/stewards (if other than the information system owner), chief information officers, senior information security officers, Inspectors General, information system security officers, users from organizations that the information system supports, and assessors.

In preparation for the assessment of security controls, the necessary background information is assembled and made available to the assessors or assessment team.[29] To the extent necessary to support the specific assessment, the organization identifies and arranges access to: (i) elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating all security policies and associated procedures for implementing policy-compliant controls; (ii) the security policies for the information system and any associated implementing procedures; (iii) individuals or groups responsible for the development, implementation, operation, and maintenance of security controls; (iv) any materials (e.g., security plans, records, schedules, assessment reports, after-action reports, agreements, authorization packages) associated with the implementation and operation of security controls; and (v) the objects to be assessed.[30] The availability of essential documentation as well as access to key organizational personnel and the information system being assessed are paramount to a successful assessment of the security controls.

Organizations consider both the *technical expertise* and level of *independence* required in selecting security control assessors. Organizations ensure that security control assessors possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls. This includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization. An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness.[31] The authorizing official or designated representative determines the required level of independence for security control assessors based on the results of the security categorization process for the information system and the ultimate risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a risk-based decision on whether to place the information system into operation or continue its operation. Independent security control assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the security control assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results.[32]

---

[29] Information system owners and organizational entities developing, implementing, and/or administering common controls (i.e., common control providers) are responsible for providing needed information to assessors.

[30] In situations where there are multiple security assessments ongoing or planned within an organization, access to organizational elements, individuals, and artifacts supporting the assessments is centrally managed by the organization to ensure a cost-effective use of time and resources.

[31] Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor(s) conducting the assessment of the security controls.

[32] The authorizing official consults with the Office of the Inspector General, the senior information security officer, and the chief information officer to discuss the implications of any decisions on assessor independence in the types of special circumstances described above.

3.2 DEVELOPING SECURITY ASSESSMENT PLANS

The *security assessment plan* provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment. The following steps are considered by assessors in developing plans to assess the security controls in organizational information systems or inherited by those systems:

- Determine which security controls/control enhancements are to be included in the assessment based upon the contents of the security plan and the purpose/scope of the assessment;
- Select the appropriate assessment procedures to be used during the assessment based on the security controls and control enhancements that are to be included in the assessment;
- Tailor the selected assessment procedures (e.g., select appropriate assessment methods and objects, assign depth and coverage attribute values);
- Develop additional assessment procedures to address any security requirements or controls that are not sufficiently covered by Special Publication 800-53;
- Optimize the assessment procedures to reduce duplication of effort (e.g., sequencing and consolidating assessment procedures) and provide cost-effective assessment solutions; and
- Finalize the assessment plan and obtain the necessary approvals to execute the plan.

3.2.1 Determine which security controls are to be assessed.

The security plan provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The assessor starts with the security controls described in the security plan and considers the purpose of the assessment. A security control assessment can be a *complete* assessment of all security controls in the information system or inherited by the system (e.g., during an initial security authorization process) or a *partial* assessment of the security controls in the information system or inherited by the system (e.g., during system development, during continuous monitoring where controls are assessed on an ongoing basis and as a result of changes affecting the controls, or where controls were previously assessed and the results accepted in the reciprocity process).[33]

For partial assessments, information system owners and common control providers collaborate with organizational officials having an interest in the assessment (e.g., senior information security officers, mission/information owners, Inspectors General, and authorizing officials) to determine which security controls are to be assessed. The selection of the security controls depends on the continuous monitoring strategy established by the information system owner or common control provider to ensure that: (i) all controls are assessed during the authorization period established by federal legislation, policies, directives, standards, and guidelines; (ii) items on the plan of action and milestones receive adequate oversight; (iii) controls with greater volatility or importance to the organization are assessed more frequently; and (iv) control implementations that have changed since the last assessment are reevaluated.[34]

[33] Partial assessments of security controls can be conducted in the initial phases of system development life cycle to promote early detection of weakness and deficiencies and a more cost-effective approach to risk mitigation.

[34] Special Publication 800-37 provides guidance on continuous monitoring as part of the risk management process.

3.2.2 Select appropriate procedures to assess the security controls.

Special Publication 800-53A, Appendix F, provides an assessment procedure for each security control and control enhancement in Special Publication 800-53. For each security control and control enhancement in the security plan to be included in the assessment, assessors select the corresponding assessment procedure from Appendix F. The selected assessment procedures vary from assessment to assessment based on the current content of the security plan and the purpose of the security assessment (e.g., complete security control assessment, partial security control assessment).

3.2.3 Tailor assessment procedures.

In a similar manner to how the security controls from Special Publication 800-53 are tailored for the organization's mission, business functions, characteristics of the information system and operating environment, organizations tailor the assessment procedures listed in Appendix F to meet specific organizational needs. Organizations have the flexibility to perform the tailoring process at the organization level for all information systems, at the individual information system level, or using a combination of organization-level and system-specific approaches. Security control assessors determine if the organization provides additional tailoring guidance prior to initiating the tailoring process. Assessment procedures are tailored by:

- Selecting the appropriate assessment methods and objects needed to satisfy the stated assessment objectives;
- Selecting the appropriate depth and coverage attribute values to define the rigor and scope of the assessment;
- Identifying common controls that have been assessed by a separately-documented security assessment plan, and do not require the repeated execution of the assessment procedures;
- Developing information system/platform-specific and organization-specific assessment procedures (which may be adaptations to those procedures in Appendix F);
- Incorporating assessment results from previous assessments where the results are deemed applicable; and
- Making appropriate adjustments in assessment procedures to be able to obtain the requisite assessment evidence from external providers.

Assessment method and object-related considerations—

It is recognized that organizations can specify, document, and configure their information systems in a variety of ways and that the content and applicability of existing assessment evidence will vary. This may result in the need to apply a variety of assessment methods to various assessment objects to generate the assessment evidence needed to determine whether the security controls are effective in their application. Therefore, the assessment methods and objects provided with each assessment procedure are termed *potential* to reflect the need to be able to choose the methods and objects most appropriate for a specific assessment. The assessment methods and objects chosen are those deemed as necessary to produce the evidence needed to make the determinations described in the determination statements. The potential methods and objects in the assessment procedure are provided as a resource to assist in the selection of appropriate methods and objects, and not with the intent to limit the selection. Organizations use their judgment in selecting from the potential assessment methods and the list of assessment objects associated with each selected method. Organizations select those methods and objects that most cost-effectively contribute to

making the determinations associated with the assessment objective.[35] The measure of the quality of assessment results is based on the soundness of the rationale provided, not the specific set of methods and objects applied. It will not be necessary, in most cases, to apply every assessment method to every assessment object to obtain the desired assessment results. And for certain assessments, it may be appropriate to employ a method not currently listed in the set of potential methods.

Depth and coverage-related considerations—

In addition to selecting appropriate assessment methods and objects, each assessment method (i.e., examine, interview, and test) is associated with depth and coverage attributes that are described in Appendix D. The attribute values identify the rigor and scope of the assessment procedures executed by the assessor. The values selected by the organization are based on the characteristics of the information system being assessed (including assurance requirements) and the specific determinations to be made. The depth and coverage attribute values are associated with the assurance requirements specified by the organization (i.e., the rigor and scope of the assessment increases in direct relationship to the assurance requirements).

Common control-related considerations—

Assessors note which security controls (or parts of security controls) in the security plan are designated as *common controls*.[36] Since the assessment of common controls is the responsibility of the organizational entity that developed and implemented the controls (i.e., common control provider), the assessment procedures in Appendix F used to assess these controls incorporate assessment results from that organizational entity. Common controls may have been previously assessed as part of the organization's information security program or as part of an information system providing common controls inherited by other organizational systems. There may also be a separate plan to assess the common controls. In either situation, information system owners coordinate the assessment of common controls with appropriate organizational officials (e.g., chief information officer, senior information security officer, mission/information owners, authorizing officials) obtaining the results of common control assessments or, if the common controls have not been assessed or are due to be reassessed, making the necessary arrangements to include or reference the common control assessment results in the current assessment.[37]

Another consideration in assessing common controls is that there are occasionally system-specific aspects of a common control that are not covered by the organizational entities responsible for the common aspects of the control. These types of security controls are referred to as *hybrid controls*. For example, CP-2, the contingency planning security control, may be deemed a hybrid control by the organization if there is a master contingency plan developed by the organization for all organizational information systems. Following up on the initial master contingency plan,

[35] The selection of assessment methods and objects (including the number and type of assessment objects) can be a significant factor in cost-effectively meeting the assessment objectives.

[36] Common controls support multiple information systems within the organization and the protection measures provided by those controls are inherited by the individual systems. Therefore, the organization determines the appropriate set of common controls to ensure that both the strength of the controls (i.e., security capability) and level of rigor and intensity of the control assessments are commensurate with the criticality and/or sensitivity of the individual information systems inheriting those controls. Weaknesses or deficiencies in common controls have the potential to adversely affect large portions of the organization and thus require significant attention.

[37] If assessment results are not currently available for the common controls, the assessment plans for the information systems under assessment that depend on those controls are duly noted. The assessments cannot be considered complete until the assessment results for the common controls are made available to information system owners.

information system owners are expected to adjust, tailor, or supplement the contingency plan as necessary, when there are system-specific aspects of the plan that need to be defined for the particular system where the control is employed. For each hybrid control, assessors include in the assessment plan, the portions of the assessment procedures from Appendix F related to the parts of the control that are system-specific to ensure that, along with the results from common control assessments, all aspects of the security control are assessed.

System/platform and organization-related considerations—

The assessment procedures in Special Publication 800-53A may be adapted to address system/platform-specific or organization-specific dependencies. This situation arises frequently in the assessment procedures associated with the security controls from the technical families in Special Publication 800-53 (i.e., access control, audit and accountability, identification and authentication, system and communications protection). For example, the assessment of a UNIX implementation of the IA-2 control for identification and authentication of users might include an explicit examination of the *.rhosts* file for UNIX systems since improper entries in that file can result in bypassing user authentication. Recent test results may also be applicable to the current assessment if those test methods provide a high degree of transparency (e.g., what was tested, when was it tested, how was it tested). Standards-based testing protocols such as the Security Content Automation Protocol (SCAP) provide an example of how organizations can help achieve this level of transparency.

Reuse of assessment evidence-related considerations—

Reuse of assessment results from previously accepted or approved assessments are considered in the body of evidence for determining overall security control effectiveness. Previously accepted or approved assessments include: (i) those assessments of common controls that are managed by the organization and support multiple information systems; or (ii) assessments of security controls that are reviewed as part of the control implementation (e.g., CP-2 requires a review of the contingency plan). The acceptability of using previous assessment results in a security control assessment is coordinated with and approved by the users of the assessment results. It is essential that information system owners and common control providers collaborate with authorizing officials and other appropriate organizational officials in determining the acceptability of using previous assessment results. When considering the reuse of previous assessment results and the value of those results to the current assessment, assessors determine: (i) the credibility of the assessment evidence; (ii) the appropriateness of previous analysis; and (iii) the applicability of the assessment evidence to current information system operating conditions. If previous assessment results are reused, the date of the original assessment and type of assessment are documented in the security assessment plan and security assessment report. It may be necessary, in certain situations, to supplement previous assessment results under consideration for reuse with additional assessment activities to fully address the assessment objectives. For example, if an independent evaluation of an information technology product did not test a particular configuration setting that is employed by the organization in an information system, then the assessor may need to supplement the original test results with additional testing to cover that configuration setting for the current information system environment. The decision to reuse assessment results is documented in the security assessment plan and the final security assessment report and is consistent with federal legislation, policies, directives, standards, and guidelines with respect to the security control assessments.

The following items are considered in validating previous assessment results for reuse:

- Changing conditions associated with security controls over time.

Security controls that were deemed effective during previous assessments may have become ineffective due to changing conditions within the information system or its environment of operation. Assessment results that were found to be previously acceptable may no longer provide credible evidence for the determination of security control effectiveness, and therefore, a reassessment would be required. Applying previous assessment results to a current assessment necessitates the identification of any changes that have occurred since the previous assessment and the impact of these changes on the previous results. For example, reusing previous assessment results from examining an organization's security policies and procedures may be acceptable if it is determined that there have not been any significant changes to the identified policies and procedures. Reusing assessment results produced during the previous authorization of an information system is a cost-effective method for supporting continuous monitoring activities and annual FISMA reporting requirements when the related controls have not changed and there are adequate reasons for confidence in their continued application.

- Amount of time that has transpired since previous assessments.

In general, as the time period between current and previous assessments increases, the credibility/utility of the previous assessment results decreases. This is primarily due to the fact that the information system or the environment in which the information system operates is more likely to change with the passage of time, possibly invalidating the original conditions or assumptions on which the previous assessment was based.

- Degree of independence of previous assessments.

Assessor independence can be a critical factor in certain types of assessments. The degree of independence required from assessment to assessment is consistent. For example, it is not appropriate to reuse results from a previous self-assessment where no assessor independence was required, in a current assessment requiring a greater degree of independence.

External information system-related considerations—

The assessment procedures in Appendix F need to be adjusted as appropriate to accommodate the assessment of external information systems.[38] Because the organization does not always have direct control over the security controls used in external information systems, or sufficient visibility into the development, implementation, and assessment of those controls, alternative assessment approaches may need to be applied, resulting in the need to tailor the assessment procedures described in Appendix F. Where required assurances of agreed-upon security controls within an information system or inherited by the system are documented in contracts or service-level agreements, assessors review these contracts or agreements and where appropriate, tailor the assessment procedures to assess either the security controls or the security control assessment results provided through these agreements. In addition, assessors take into account any other assessments that have been conducted, or are in the process of being conducted, for external information systems that are relied upon with regard to protecting the information system under

[38] An *external information system* is an information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. Special Publications 800-37 and 800-53 provide additional guidance on external information systems and the effect of employing security controls in those types of environments.

assessment. Applicable information from these assessments, if deemed reliable, is incorporated into the security assessment report.

3.2.4 Develop assessment procedures for organization-specific security controls.

Based on organizational policies, mission or business function requirements, and an assessment of risk, organizations may choose to develop and implement additional (organization-specific) security controls or control enhancements for their information systems that are beyond the scope of Special Publication 800-53. Such security controls are documented in the security plan for the information system as controls not found in Special Publication 800-53. To assess the security controls in this situation, assessors use the guidelines in Chapter Two to develop assessment procedures for those controls and control enhancements. The assessment procedures developed are subsequently integrated into the security assessment plan.

3.2.5 Optimize selected assessment procedures to ensure maximum efficiency.

Assessors have a great deal of flexibility in organizing a security assessment plan that meets the needs of the organization and that provides the best opportunity for obtaining the necessary evidence to determine security control effectiveness, while reducing overall assessment costs. Combining and consolidating assessment procedures is one area where this flexibility can be applied. During the assessment of an information system, assessment methods are applied numerous times to a variety of assessment objects within a particular family of security controls. To save time, reduce assessment costs, and maximize the usefulness of assessment results, assessors review the selected assessment procedures for the security control families and combine or consolidate the procedures (or parts of procedures) whenever possible or practicable. For example, assessors may wish to consolidate interviews with key organizational officials dealing with a variety of security-related topics. Assessors may have other opportunities for significant consolidations and cost savings by examining all security policies and procedures from the eighteen families of security controls at the same time or organizing groups of related policies and procedures that could be examined as a unified entity. Obtaining and examining configuration settings from similar hardware and software components within the information system is another example that can provide significant assessment efficiencies.

An additional area for consideration in optimizing the assessment process is the sequence in which security controls are assessed. The assessment of some security controls before others may provide information that facilitates understanding and assessment of other controls. For example, security controls such as CM-2 (Baseline Configuration), CM-8 (Information System Component Inventory), PL-2 (System Security Plan), RA-2 (Security Categorization), and RA-3 (Risk Assessment) produce general descriptions of the information system. Assessing these security controls early in the assessment process may provide a basic understanding of the information system that can aid in assessing other security controls. The supplemental guidance of many security controls also identifies related controls that can provide useful information in organizing the assessment procedures.[39] For example, AC-19 (Access Control for Portable and Mobile Devices) lists security controls MP-4 (Media Storage) and MP-5 (Media Transport) as being related to AC-19. Since AC-19 is related to MP-4 and MP-5, the sequence in which assessments are conducted for AC-19, MP-4, and MP-5 may facilitate the reuse of assessment information from one control in assessing other related controls.

[39] Security control assessment sequencing is also addressed in the assessment cases described in Appendix H.

3.2.6 Finalize security assessment plan and obtain approval to execute plan.

After selecting the assessment procedures (including developing necessary procedures not contained in the Special Publication 800-53A catalog of procedures), tailoring the procedures for information system/platform-specific and organization-specific conditions, optimizing the procedures for efficiency, and addressing the potential for unexpected events impacting the assessment, the assessment plan is finalized and the schedule is established including key milestones for the assessment process. Once the security assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials[40] to ensure that the plan is complete, consistent with the security objectives of the organization and the organization's assessment of risk, and cost-effective with regard to the resources allocated for the assessment.

3.3 CONDUCTING SECURITY CONTROL ASSESSMENTS

After the security assessment plan is approved by the organization, the assessor or assessment team executes the plan in accordance with the agreed-upon schedule. Determining the size and organizational makeup of the security assessment team (i.e., skill sets, technical expertise, and assessment experience of the individuals composing the team) is part of the risk management decisions made by the organization requesting and initiating the assessment.

The output and end result of the security control assessment is the *security assessment report*, which documents the assurance case for the information system and is one of three key documents in the security authorization package developed by information system owners and common control providers for authorizing officials.[41] The security assessment report includes information from the assessor (in the form of assessment findings) necessary to determine the effectiveness of the security controls employed within or inherited by the information system. The security assessment report is an important factor in an authorizing official's determination of risk. Organizations may choose to develop an assessment *summary* from the detailed findings that are generated by the assessor during the security control assessment. An assessment summary can provide an authorizing official with an abbreviated version a of *Security Assessment Report* focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls. Appendix G provides additional information on the recommended content of security assessment reports.

Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement contained within an assessment procedure executed by an assessor produces one of the following findings: (i) *satisfied (S)*; or (ii) *other than satisfied (O)*. A finding of satisfied indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) indicates that the assessment objective for the control has been met producing a fully acceptable result. A finding of other than satisfied indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the control that may need to be addressed by the organization. A finding of other than satisfied may

[40] Organizations establish a security assessment plan approval process with the specific organizational officials (e.g., information systems owners, common control providers, information system security officers, senior information security officers, authorizing officials) designated as approving authorities.

[41] In accordance with Special Publication 800-37, the security authorization package consists of the security plan (including the risk assessment), the security assessment report, and the plan of action and milestones (POAM).

also indicate that for reasons specified in the assessment report, the assessor was unable to obtain sufficient information to make the particular determination called for in the determination statement. For assessment findings that are *other than satisfied*, organizations may choose to define *subcategories* of findings indicating the severity and/or criticality of the weaknesses or deficiencies discovered and the potential adverse effects on organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Defining such subcategories can help to establish priorities for needed risk mitigation actions.

Assessor findings are an unbiased, factual reporting of what was found concerning the security control assessed. For each finding of other than satisfied, assessors indicate which parts of the security control are affected by the finding (i.e., aspects of the control that were deemed not satisfied or were not able to be assessed) and describe how the control differs from the planned or expected state. The potential for compromises to confidentiality, integrity, and availability due to *other than satisfied* findings are also noted by the assessor in the security assessment report. This notation reflects the lack of a specified protection and the exploitation that could occur as a result (i.e. workstation, dataset, root level access). Risk determination and acceptance activities are conducted by the organization post assessment as part of the risk management strategy established by the organization. These risk management activities involve the senior leadership of the organization including for example, heads of agencies, mission/business owners, information owners/stewards, risk executive (function), and authorizing officials, in consultation with appropriate organizational support staff (e.g., senior information security officers, chief information officers, information system owners, common control providers, and assessors). Security control assessment results are documented at the level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational policy, NIST guidelines, and OMB policy. The reporting format is appropriate for the type of security control assessment conducted (e.g., self-assessments by information system owners and common control providers, independent verification and validation, independent assessments supporting the security authorization process, or independent audits or inspections).

Information system owners and common control providers rely on the security expertise and the technical judgment of assessors to: (i) assess the security controls in the information system and inherited by the system; and (ii) provide recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessment results produced by the assessor (i.e., findings of *satisfied* or *other than satisfied*, identification of the parts of the security control that did not produce a satisfactory result, and a description of resulting potential for compromises to the information system or its environment of operation) are provided to information system owners and common control providers in the initial security assessment report. System owners and common control providers may choose to act on selected recommendations of the assessor before the security assessment report is finalized if there are specific opportunities to correct weaknesses or deficiencies in security controls or to correct and/or clarify misunderstandings or interpretations of assessment results.[42] Security controls that

[42] The correction of weaknesses or deficiencies in security controls or carrying out of selected recommendations during the review of the initial security assessment report by information system owners or common control providers is not intended to replace the formal risk mitigation process by the organization which occurs after the delivery of the final report. Rather, it provides the information system owner or common control provider with an opportunity to address weaknesses or deficiencies that may be quickly corrected. However, in situations where limited resources exist for remediating weaknesses and deficiencies discovered during the security control assessment, organizations may decide without prejudice that waiting for the risk assessment to prioritize remediation efforts is the better course of action.

are modified, enhanced, or added during this process are reassessed by the assessor prior to the production of the final security assessment report.

3.4 ANALYZING SECURITY ASSESSMENT REPORT RESULTS

Since results of the security control assessment ultimately influence the content of the security plan and the plan of action and milestones, information system owners and common control providers review the security assessment report and the updated risk assessment and with the concurrence of designated organizational officials (e.g., authorizing officials, chief information officer, senior information security officer, mission/information owners), determine the appropriate steps required to correct weaknesses and deficiencies identified during the assessment. By using the labels of *satisfied* and *other than satisfied*, the reporting format for the assessment findings provides visibility for organizational officials into specific weaknesses and deficiencies in security controls within the information system or inherited by the system and facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities. For example, information system owners or common control providers in consultation with designated organizational officials, may decide that certain assessment findings marked as other than satisfied are of an inconsequential nature and present no significant risk to the organization. Conversely, system owners or common control providers may decide that certain findings marked as other than satisfied are significant, requiring immediate remediation actions. In all cases, the organization reviews each assessor finding of other than satisfied and applies its judgment with regard to the severity or seriousness of the finding and whether the finding is significant enough to be worthy of further investigation or remedial action.

Senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources first to the information systems that are supporting the most critical and sensitive missions for the organization or correcting the deficiencies that pose the greatest degree of risk. Ultimately, the security control assessment findings and any subsequent mitigation actions (informed by the updated risk assessment) initiated by information system owners or common control providers in collaboration with designated organizational officials trigger updates to the key documents used by authorizing officials to determine the security status of the information system and its suitability for authorization to operate. These documents include the security plan with updated risk assessment, security assessment report, and plan of action and milestones.

Figure 1 provides an overview of the security control assessment process including the activities carried out during pre-assessment, assessment, and post-assessment.

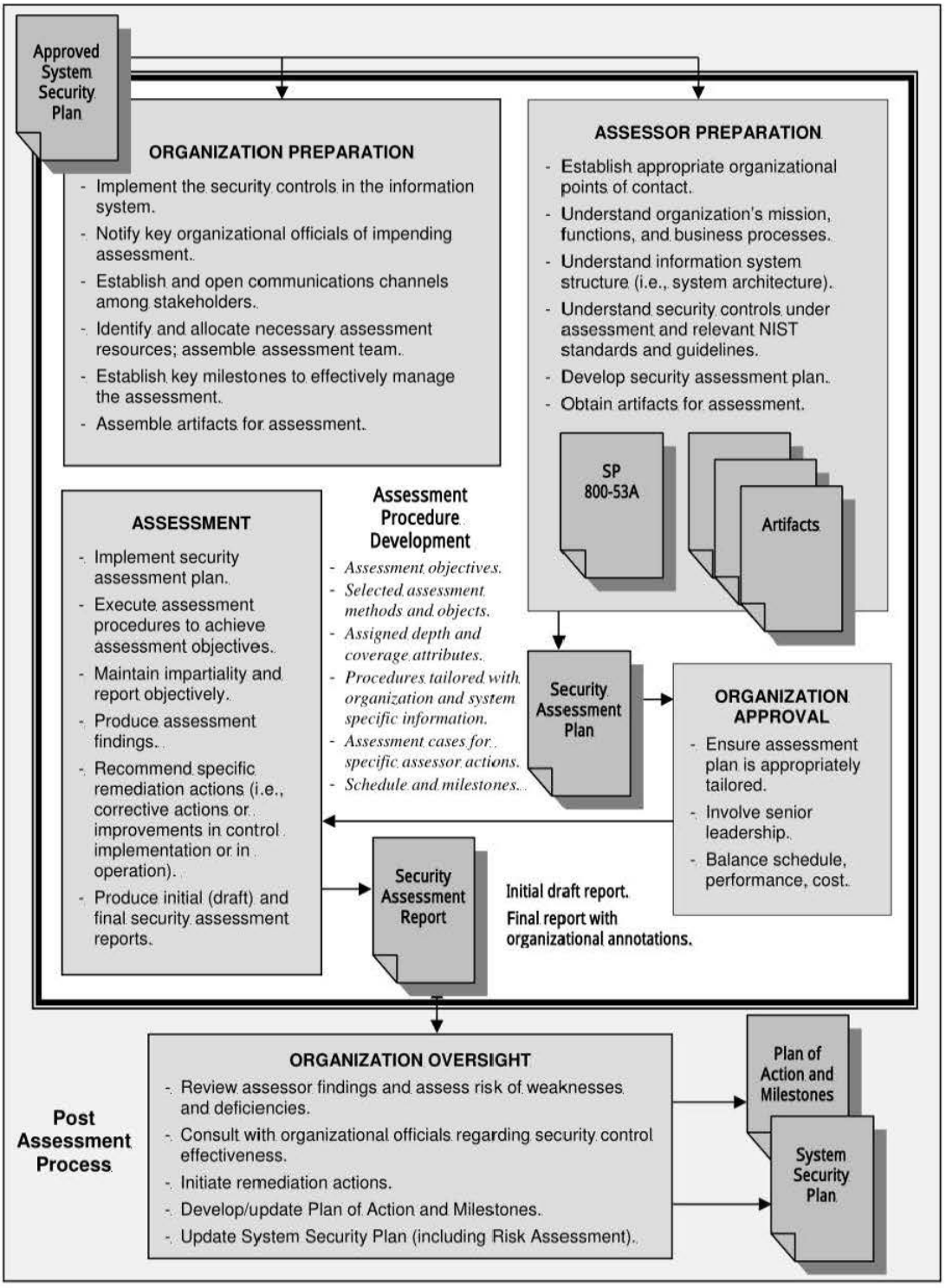


FIGURE 1: SECURITY CONTROL ASSESSMENT PROCESS OVERVIEW

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, INSTRUCTIONS, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

POLICIES, DIRECTIVES, INSTRUCTIONS

1. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, April 2010.
2. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.
3. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
4. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

STANDARDS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
3. ISO/IEC 15408:2005, *Common Criteria for Information Technology Security Evaluation*, 2005.

GUIDELINES

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
2. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
3. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
4. National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.
5. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

6. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

7. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

8. National Institute of Standards and Technology Special Publication 800-126, Revision 1 (Draft), *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0*, May 2010.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used within Special Publication 800-53A. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See *Executive Agency*.
Assessment	See *Security Control Assessment*.
Assessment Findings	Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition.
Assessment Method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.
Assessment Object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
Assessment Objective	A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.
Assessment Procedure	A set of assessment *objectives* and an associated set of assessment *methods* and assessment *objects*.
Assessor	See *Security Control Assessor*.
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application.
Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.

FTC-0002381

Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary [NIST SP 800-37]	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorizing Official [NIST SP 800-37]	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative [NIST SP 800-37]	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Basic Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.
Black Box Testing	See *Basic Testing*.

Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	See *Senior Agency Information Security Officer*.
Common Control [NIST SP 800-37]	A security control that is inherited by one or more organizational information systems. See *Security Control Inheritance*.
Common Control Provider [NIST SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).
Compensating Security Controls [NIST SP 800-53]	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253, that provide equivalent or comparable protection for an information system.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Controlled Unclassified Information	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces *Sensitive But Unclassified (SBU)*.

Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Federal Agency	See *Executive Agency*.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing.
Gray Box Testing	See *Focused Testing*.
Hybrid Security Control [NIST SP 800-53]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.

Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Program Plan [NIST SP 800-53]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Boundary	See *Authorization Boundary*.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
Information System-related Security Risks	Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.

Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Reciprocity	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Risk [CNSSI 4009]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.]
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Executive (Function) [NIST SP 800-37]	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management [CNSSI 4009]	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Security Authorization	See *Authorization*.

Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Controls [FIPS 199, CNSSI 4009]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis [NIST SP 800-37]	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.

Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.]
Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplementation (Assessment Procedures)	The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.
Supplementation (Security Controls)	The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.
System	See *Information System*.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system.

Tailoring [NIST SP 800-53, CNSSI 4009]	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Tailoring (Assessment Procedures)	The process by which assessment procedures defined in Special Publication 800-53A are adjusted, or scoped, to match the characteristics of the information system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly-constrained assessment approaches.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.
Threat [CNSSI 4009]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
White Box Testing	See *Comprehensive Testing*.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
POAM	Plan of Action and Milestones
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SP	Special Publication
U.S.C.	United States Code
VoIP	Voice over Internet Protocol

APPENDIX D

ASSESSMENT METHOD DESCRIPTIONS

ASSESSMENT METHOD DEFINITIONS, APPLICABLE OBJECTS, AND ATTRIBUTES

This appendix defines the three assessment methods that can be used by assessors during security control assessments: (i) *examine*; (ii) *interview*; and (iii) *test*. Included in the definition of each assessment method are types of objects to which the method can be applied. The application of each method is described in terms of the attributes of *depth* and *coverage*, progressing from *basic* to *focused* to *comprehensive*. The attribute values correlate to the assurance requirements specified by the organization.[43] The depth attribute addresses the rigor and level of detail of the assessment. For the depth attribute, the *focused* attribute value includes and builds upon the assessment rigor and level of detail defined for the *basic* attribute value; the *comprehensive* attribute value includes and builds upon the assessment rigor and level of detail defined for the *focused* attribute value. The coverage attribute addresses the scope or breadth of the assessment. For the coverage attribute, the *focused* attribute value includes and builds upon the number and type of assessment objects defined for the *basic* attribute value; the *comprehensive* attribute value includes and builds upon the number and type of assessment objects defined for the *focused* attribute value. The use of **bolded text** in the assessment method description indicates the content that was added to and appears for the first time, in the description indicating greater rigor and detail for the attribute value.

[43] For other than national security systems, organizations meet minimum assurance requirements specified in Special Publication 800-53, Appendix E.

ASSESSMENT METHOD: Examine

ASSESSMENT OBJECTS: Specifications (e.g., policies, plans, procedures, system requirements, designs)
Mechanisms (e.g., functionality implemented in hardware, software, firmware)
Activities (e.g., system operations, administration, management; exercises).

DEFINITION: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations, reviewing the results of contingency plan exercises; observing incident response activities; studying technical manuals and user/administrator guides; checking, studying, or observing the operation of an information technology mechanism in the information system hardware/software; or checking, studying, or observing physical security measures related to the operation of an information system.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: (i) *basic*; (ii) *focused*; and (iii) *comprehensive*.
  - Basic examination: Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation (e.g., functional-level descriptions for mechanisms; high-level process descriptions for activities; and actual documents for specifications). Basic examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.
  - Focused examination: Examination that consists of high-level reviews, checks, observations, or inspections **and more in depth studies/analyses** of the assessment object. This type of examination is conducted using a **substantial** body of evidence or documentation (e.g., functional-level descriptions **and where appropriate and available, high-level design information** for mechanisms; high-level process descriptions **and implementation procedures** for activities; and the actual documents **and related documents** for specifications). **Focused** examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Comprehensive examination: Examination that consists of high-level reviews, checks, observations, or inspections and more in depth, **detailed, and thorough** studies/analyses of the assessment object. This type of examination is conducted using an **extensive** body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information, **low-level design information, and implementation information** for mechanisms; high-level process descriptions and **detailed** implementation procedures for activities; and the actual documents and related documents for specifications[44]). **Comprehensive** examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

[44] While additional documentation is likely for mechanisms when moving from basic to focused to comprehensive examinations, the documentation associated with specifications and activities may be the same or similar for focused and comprehensive examinations, with the rigor of the examinations of these documents being increased at the comprehensive level.

- The *coverage* attribute addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined, the number of objects to be examined (by type), and specific objects to be examined.[45] There are three possible values for the coverage attribute: (i) *basic*, (ii) *focused*, and (iii) *comprehensive*.
  - Basic examination: Examination that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.
  - Focused examination: Examination that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Comprehensive examination: Examination that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

[45] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific objects to be examined for the particular attribute value described.

ASSESSMENT METHOD: Interview

ASSESSMENT OBJECTS: Individuals or groups of individuals.

DEFINITION: The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example, interviewing agency heads, chief information officers, senior agency information security officers, authorizing officials, information owners, information system and mission owners, information system security officers, information system security managers, personnel officers, human resource managers, facilities managers, training officers, information system operators, network and system administrators, site managers, physical security officers, and users.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: (i) *basic*; (ii) *focused*; and (iii) *comprehensive*.
  - Basic interview: Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Basic interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.
  - Focused interview: Interview that consists of broad-based, high-level discussions **and more in depth discussions in specific areas** with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions **and more in depth questions in specific areas where responses indicate a need for more in depth investigation**. **Focused** interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Comprehensive interview: Interview that consists of broad-based, high-level discussions and more in depth, **probing** discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in depth, **probing** questions in specific areas where responses indicate a need for more in depth investigation. **Comprehensive** interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.
- The *coverage* attribute addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed (by organizational role and associated responsibility), the number of individuals to be interviewed (by type), and specific individuals to be interviewed.[46] There are three possible values for the coverage attribute: (i) *basic*, (ii) *focused*; and (iii) *comprehensive*.
  - Basic interview: Interview that uses a representative sample of individuals in key organizational roles to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.
  - Focused interview: Interview that uses a representative sample of individuals in key organizational roles **and other specific individuals deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.

[46] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific individuals to be interviewed for the particular attribute value described.

- Comprehensive interview: Interview that uses a **sufficiently large** sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

ASSESSMENT METHOD: Test

ASSESSMENT OBJECTS: Mechanisms (e.g., hardware, software, firmware)
Activities (e.g., system operations, administration, management; exercises)

DEFINITION: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.[47]

SUPPLEMENTAL GUIDANCE: Typical assessor actions may include, for example: testing access control, identification and authentication, and audit mechanisms; testing security configuration settings; testing physical access control devices; conducting penetration testing of key information system components; testing information system backup operations; testing incident response capability; and exercising contingency planning capability.

ATTRIBUTES: Depth, Coverage

- The *depth* attribute addresses the types of testing to be conducted. There are three possible values for the depth attribute: (i) *basic* testing; (ii) *focused* testing; and (iii) *comprehensive* testing.
  - Basic testing: Test methodology (also known as *black box* testing) that assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Basic testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors.
  - Focused testing: Test methodology (also known as *gray box* testing) that assumes **some** knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification **and limited system architectural information (e.g., high-level design)** for mechanisms and a high-level process description **and high-level description of integration into the operational environment** for activities. Focused testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
  - Comprehensive testing: Test methodology (also known as *white box* testing) that assumes **explicit and substantial** knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, **extensive** system architectural information (e.g., high-level design, **low-level design) and implementation representation (e.g., source code, schematics)** for mechanisms and a high-level process description and **detailed** description of integration into the operational environment for activities. Comprehensive testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.
- The *coverage* attribute addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested, the number of objects to be tested (by type), and specific objects to be tested.[48] There are three possible values for the coverage attribute: (i) *basic*; (ii) *focused*; and (iii) *comprehensive*.

[47] Testing is typically used to determine if mechanisms or activities meet a set of predefined specifications. Testing can also be performed to determine characteristics of a security control that are not commonly associated with predefined specifications, with an example of such testing being penetration testing. Guidelines for conducting penetration testing are provided in Appendix E.

[48] The organization, considering a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors and provides direction on the type, number, and specific objects to be tested for the particular attribute value described. For mechanism-related testing, the coverage attribute also addresses the extent of the testing conducted (e.g., for software, the number of test cases and modules tested; for hardware, the range of inputs, number of components tested, and range of environmental factors over which the testing is conducted).

- Basic testing: Testing that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors.
- Focused testing: Testing that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors **and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended**.
- Comprehensive testing: Testing that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are **further** increased grounds for confidence that the control is implemented correctly and operating as intended **on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control**.

APPENDIX E

PENETRATION TESTING

ASSESSMENT TOOLS AND TECHNIQUES TO IDENTIFY INFORMATION SYSTEM WEAKNESSES

Organizations should consider adding controlled penetration testing to their arsenal of tools and techniques used to assess the security controls in organizational information systems. Penetration testing is a specific type of assessment in which assessors simulate the actions of a given class of attacker by using a defined set of documentation (that is, the documentation representative of what that class of attacker is likely to possess) and working under other specific constraints to attempt to circumvent the security features of an information system. Penetration testing is conducted as a controlled attempt to breach the security controls employed within the information system using the attacker's techniques and appropriate hardware and software tools. Penetration testing represents the results of a specific assessor or group of assessors at a specific point in time using agreed-upon *rules of engagement*. Considering the complexity of the information technologies commonly employed by organizations today, penetration testing should be viewed not as a means to verify the security of an information system, but rather as a means to: (i) enhance the organization's understanding of the system; (ii) uncover weaknesses or deficiencies in the system; and (iii) indicate the level of effort required on the part of adversaries to breach the system safeguards.

Penetration testing exercises can be scheduled and/or random in accordance with organizational policy and organizational assessments of risk. Consideration should be given to performing penetration tests: (i) on any newly developed information system (or legacy system undergoing a major upgrade) before the system is authorized for operation; (ii) after important changes are made to the environment in which the information system operates; and (iii) when a new type of attack is discovered that may impact the system. Organizations actively monitor the information systems environment and the threat landscape (e.g., new vulnerabilities, attack techniques, new technology deployments, user security awareness and training) to identify changes that require out-of-cycle penetration testing.

Organizations specify which components within the information system are subject to penetration testing and the attacker's profile to be adopted throughout the penetration testing exercises. Organizations train selected personnel in the use and maintenance of penetration testing tools and techniques. Effective penetration testing tools should have the capability to readily update the list of attack techniques and exploitable vulnerabilities used during the exercises. Organizations should update the list of attack techniques and exploitable vulnerabilities used in penetration testing in accordance with an organizational assessment of risk or when significant new vulnerabilities or threats are identified and reported. Whenever possible, organizations should employ tools and attack techniques that include the capability to perform penetration testing exercises on information systems and security controls in an automated manner.

The information obtained from the penetration testing process should be shared with appropriate personnel throughout the organization to help prioritize the vulnerabilities in the information system that are demonstrably subject to compromise by attackers of a profile equivalent to the ones used in the penetration testing exercises. The prioritization helps to determine effective strategies for eliminating the identified vulnerabilities and mitigating associated risks to the organization's operations and assets, to individuals, to other organizations, and to the Nation resulting from the operation and use of the information system. Penetration testing should be

FTC-0002401

integrated into the network security testing process and the patch and vulnerability management process. Special Publication 800-40 provides guidance on patch and vulnerability management. Special Publication 800-42 provides guidance on network security testing. Special Publication 800-115 provides guidance on information security testing.

Penetration Testing Considerations

Organizations consider the following criteria in developing and implementing a controlled penetration testing program. An effective penetration test:

- Goes beyond vulnerability scanning, to provide an explicit and often dramatic proof of mission risks and an indicator of the level of effort an adversary would need to expend in order to cause harm to the organization's operations and assets, to individuals, to other organizations, or to the Nation;
- Approaches the information system as the adversary would, considering vulnerabilities, incorrect system configurations, trust relationships between organizations, and architectural weaknesses in the environment under test;
- Has a clearly defined scope and contains as a minimum:
  - A definition of the environment subject to test (e.g., facilities, users, organizational groups, etc.);
  - A definition of the attack surface to be tested (e.g., servers, desktop systems, wireless networks, Web applications, intrusion detection and prevention systems, firewalls, email accounts, user security awareness and training posture, incident response posture, etc.);
  - A definition of the threat sources to simulate (e.g., an enumeration of attacker's profiles to be used: internal attacker, casual attacker, single or group of external targeted attackers, criminal organization, etc.);
  - A definition of level of effort (time and resources) to be expended; and
  - A definition of the rules of engagement.
- Thoroughly documents all activities performed during the test, including all exploited vulnerabilities, and how the vulnerabilities were combined into attacks;
- Produces results indicating a likelihood of occurrence for a given attacker by using the level of effort the team needed to expend in penetrating the information system as an indicator of the penetration resistance of the system;
- Validates existing security controls (including risk mitigation mechanisms such as firewalls, intrusion detection and prevention systems);
- Provides a verifiable and reproducible log of all the activities performed during the test; and
- Provides actionable results with information about possible remediation measures for the successful attacks performed.

APPENDIX F

ASSESSMENT PROCEDURE CATALOG

OBJECTIVES, METHODS, AND OBJECTS FOR ASSESSING SECURITY CONTROLS

This appendix provides a catalog of procedures to assess the security controls and control enhancements in Special Publication 800-53.[49] Assessors select assessment procedures from the catalog in accordance with the guidance provided in Section 3.2. Since the contents of the security plan affect the development of the security assessment plan and the assessment, there will likely be assessment procedures in the catalog that assessors will not use because: (i) the associated security controls or control enhancements are not contained in the security plan for the information system;[50] or (ii) the security controls or control enhancements are not being assessed at this particular time (e.g., during an assessment of a subset of the controls as part of continuous monitoring activities).

The same assessment object may appear in multiple object lists in a variety of assessment procedures. The same object may be used in multiple contexts to obtain needed information or evidence for a particular aspect of an assessment. Assessors use the general references as appropriate to obtain the necessary information to make the specified determinations required by the assessment objective. For example, a reference to access control policy appears in the assessment procedures for AC-2 and AC-7. For assessment procedure AC-2, assessors use the access control policy to find information about that portion of the policy that addresses account management for the information system. For assessment procedure AC-7, assessors use the access control policy to find information about that portion of the policy that addresses unsuccessful login attempts for the information system.

Assessors are responsible for combining and consolidating the assessment procedures whenever possible or practical. Optimizing assessment procedures can save time, reduce assessment costs, and maximize the usefulness of assessment results. Assessors optimize assessment procedures by determining the best sequencing of the procedures. The assessment of some security controls before others may provide information that facilitates understanding and assessment of other controls.

[49] In the event of any differences between the assessment objectives identified for assessing the security controls and the underlining intent expressed by the security control statements defined in the most recent version of Special Publication 800-53, Special Publication 800-53 remains the definitive expression of the control or enhancement.

[50] The execution of the RMF includes the selection of an initial set of security controls employed within or inherited by an organizational information system followed by a control *tailoring* and *supplementation* process. The tailoring and supplementation process will likely change the set of security controls that will be contained in the final security plan. Therefore, the selection of assessment procedures from the catalog of available procedures is based solely on the content of the security plan after the tailoring and supplementation activities are completed.

Implementation Tips

TIP #1: Select only those assessment procedures from Appendix F that correspond to the security controls and control enhancements in the *approved security plan* and that are to be included in the assessment.

TIP #2: The assessment procedures selected from Appendix F are simply *example* procedures that serve as a starting point for organizations preparing for assessments. These assessment procedures are tailored and supplemented as necessary, in accordance with the guidance in Section 3.2 to adapt the procedures to specific organizational requirements and operating environments.

TIP #3: With respect to the *assessment procedures* in Appendix F, assessors need apply only those procedures, methods, and objects necessary for making a final determination that a particular security control objective is satisfied or not satisfied (see Section 3.3).

TIP #4: Assessors apply to each assessment method, values for depth and coverage (described in Appendix D) that are commensurate with the characteristics of the information system (including assurance requirements) and the specific assessment activity that supports making a determination of the effectiveness of the security controls under review. The values selected for the depth and coverage attributes indicate the relative effort required in applying an assessment method to an assessment object (i.e., the rigor and scope of the activities associated with the assessment). The depth and coverage attributes, while not repeated in every assessment procedure in this appendix, can be represented as follows:

Interview: [*ASSIGN ATTRIBUTE VALUES:* <depth>, <coverage>].
[*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

TIP #5: Assessors may find useful assessment-related information in the Supplemental Guidance section of each security control described in Special Publication 800-53. This information can be used to carry out more effective assessments with regard to the application of assessment procedures.

Note: When assessing agency compliance with NIST guidance, auditors, Inspectors General, evaluators, and/or assessors consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

REMINDER

Whereas a set of potential assessment methods have been included in the following catalog of assessment procedures, these are not intended to be mandatory or exclusive and, depending on the particular circumstances of the information system to be assessed, not all methods may be required or other assessment methods may also be used. In addition, the potential assessment objects listed are not intended to be a mandatory set, but rather a set from which the necessary and sufficient set of objects for a given assessment can be selected to make the appropriate determinations. For specific recommendations regarding current best practices for security control assessments, organizations can consult the assessment case development project described in Appendix H and the assessment cases listed on the NIST Web site.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-1	**ACCESS CONTROL POLICY AND PROCEDURES**
AC-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents access control policy;* *(ii) the organization access control policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;* *(iv) the organization develops and formally documents access control procedures;* *(v) the organization access control procedures facilitate implementation of the access control policy and associated access controls; and* *(vi) the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access control responsibilities].
AC-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of access control policy reviews/updates;* *(ii) the organization reviews/updates access control policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of access control procedure reviews/updates; and* *(iv) the organization reviews/updates access control procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access control responsibilities].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-2	**ACCOUNT MANAGEMENT**

AC-2.1	**ASSESSMENT OBJECTIVE:**
	Determine if:
	(i) the organization manages information system accounts, including:
	- *identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);*
	- *establishing conditions for group membership;*
	- *identifying authorized users of the information system and specifying access privileges;*
	- *requiring appropriate approvals for requests to establish accounts;*
	- *establishing, activating, modifying, disabling, and removing accounts;*
	- *specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;*
	- *notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;*
	- *deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and*
	- *granting access to the system based on:*
	  - *a valid access authorization;*
	  - *intended system usage; and*
	  - *other attributes as required by the organization or associated missions/business functions; and*
	(ii) the organization defines the frequency of information system account reviews; and
	(iii) the organization reviews information system accounts in accordance with organization-defined frequency.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
	Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records].
	Interview: [*SELECT FROM:* Organizational personnel with account management responsibilities].

AC-2(1)	ACCOUNT MANAGEMENT
AC-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to support information system account management functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(2)	ACCOUNT MANAGEMENT
AC-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a time period for each type of account after which the information system terminates temporary and emergency accounts; and* *(ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(3)	ACCOUNT MANAGEMENT
AC-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines in a time period after which the information system disables inactive accounts; and* *(ii) the information system automatically disables inactive accounts after organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(4)	ACCOUNT MANAGEMENT
AC-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system automatically audits:* - *account creation;* - *modification;* - *disabling; and* - *termination actions; and* *(ii) the information system notifies, as required, appropriate individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(5)	ACCOUNT MANAGEMENT
AC-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of expected inactivity and/or description of when users log out;* *(ii) the organization requires that users log out in accordance with the organization-defined time-period of inactivity and/or description of when to log out;* *(iii) the organization determines normal time-of-day and duration usage for information system accounts;* *(iv) the organization monitors for atypical usage of information system accounts; and* *(v) the organization reports atypical usage to designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; security violation reports; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities].

AC-2(6)	ACCOUNT MANAGEMENT
AC-2(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system dynamically manages user privileges and associated access authorizations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing account management functions].

AC-2(7)	ACCOUNT MANAGEMENT
AC-2(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and* *(ii) the organization tracks and monitors privileged role assignments.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-3	**ACCESS ENFORCEMENT**
AC-3.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access enforcement policy].

AC-3(1)	**ACCESS ENFORCEMENT** [Withdrawn: Incorporated into AC-6].
AC-3(1).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into AC-6]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into AC-6].

AC-3(2)	**ACCESS ENFORCEMENT**
AC-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines, in organizational policies and procedures, the privileged commands for which dual authorization is to be enforced; and* *(ii) the information system enforces dual authorization based on organizational policies and procedures for organization-defined privileged commands.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement and dual authorization; security plan; information system design documentation; information system configuration settings and associated documentation; list of privileged commands requiring dual authorization; list of approved authorizations (user privileges); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access enforcement responsibilities]. **Test**: [*SELECT FROM:* Dual authorization mechanisms implementing access control policy].

AC-3(3)	ACCESS ENFORCEMENT
AC-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the users and resources over which the information system is to enforce nondiscretionary access control policies;* *(ii) the organization defines nondiscretionary access control policies to be enforced over the organization-defined set of users and resources, where the rule set for each policy specifies:* – *access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and* – *required relationships among the access control information to permit access; and* *(iii) the information system enforces organization-defined nondiscretionary access control policies over the organization-defined set of users and resources.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; nondiscretionary access control policies; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; list of users and resources requiring enforcement of nondiscretionary access control policies; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access enforcement responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing nondiscretionary access control policy].

AC-3(4)	ACCESS ENFORCEMENT
AC-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces a Discretionary Access Control (DAC) policy that:* – *allows users to specify and control sharing by named individuals or groups of individuals, or by both;* – *limits propagation of access rights; and* – *includes or excludes access to the granularity of a single user.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; discretionary access control policy; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing discretionary access control policy].

AC-3(5)	ACCESS ENFORCEMENT
AC-3(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security-relevant information to which the information system prevents access except during secure, nonoperable system states; and* *(ii) the information system prevents access to organization-defined security-relevant information except during secure, nonoperable system states.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access enforcement responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms preventing access to security-relevant information within the information system].

AC-3(6)	ACCESS ENFORCEMENT
AC-3(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the user and/or system information to be encrypted or stored off-line in a secure location; and* *(ii) the organization encrypts, or stores off-line in a secure location, organization-defined user and/or system information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with access enforcement responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access enforcement functions].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-4	**INFORMATION FLOW ENFORCEMENT**
AC-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines applicable policy for controlling the flow of information within the system and between interconnected systems;* *(ii) the organization defines approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy; and* *(iii) the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(1)	INFORMATION FLOW ENFORCEMENT
AC-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(2)	INFORMATION FLOW ENFORCEMENT
AC-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(3)	INFORMATION FLOW ENFORCEMENT
AC-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines policy that allows or disallows information flows based on changing conditions or operational consideration; and* *(ii) the information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(4)	INFORMATION FLOW ENFORCEMENT
AC-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents encrypted data from bypassing content-checking mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(5)	INFORMATION FLOW ENFORCEMENT
AC-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the limitations on the embedding of data types with other data types; and* *(ii) the information system enforces organization-defined limitations on the embedding of data types within other data types.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(6)	INFORMATION FLOW ENFORCEMENT
AC-4(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces information flow control on metadata.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(7)	INFORMATION FLOW ENFORCEMENT
AC-4(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the one-way information flows to be enforced by the information system; and* *(ii) the information system enforces organization-defined one-way information flows using hardware mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Hardware mechanisms implementing information flow enforcement policy].

AC-4(8)	INFORMATION FLOW ENFORCEMENT
AC-4(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security policy filters to be enforced by the information system; and* *(ii) the information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; list of security policy filters; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(9)	INFORMATION FLOW ENFORCEMENT
AC-4(9).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security policy filters that the information system enforces for the use of human review; and* *(ii) the information system enforces the use of human review for the organization-defined security policy filters, when the system is not capable of making an information flow control decision.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for making information flow control decisions when the information system is not capable of doing so].

AC-4(10)	INFORMATION FLOW ENFORCEMENT
AC-4(10).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security policy filters that privileged administrators have the capability to enable/disable; and* *(ii) the information system provides the capability for a privileged administrator to enable/disable organization-defined security policy filters.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for enabling/disabling security policy filters]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

FTC-0002417

AC-4(11)	INFORMATION FLOW ENFORCEMENT
AC-4(11).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security policy filters that privileged administrators have the capability to configure; and* *(ii) the information system provides the capability for a privileged administrator to configure organization-defined security policy filters to support different security policies.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for configuring security policy filters]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(12)	INFORMATION FLOW ENFORCEMENT
AC-4(12).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, when transferring information between different security domains, identifies information flows by data type specification and usage.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(13)	INFORMATION FLOW ENFORCEMENT
AC-4(13).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(14)	INFORMATION FLOW ENFORCEMENT
AC-4(14).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security policy requirements for constraining data structure and content; and* *(ii) the information system, when transferring information between different security domains, implements policy filters that constrain data structure and content in accordance with organization-defined information security policy requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; list of policy filters; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(15)	INFORMATION FLOW ENFORCEMENT
AC-4(15).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system, when transferring information between different security domains, detects unsanctioned information; and* *(ii) the information system prohibits the transfer of unsanctioned information in accordance with the security policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(16)	INFORMATION FLOW ENFORCEMENT
AC-4(16).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system enforces security policies regarding information on interconnected systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

AC-4(17)	INFORMATION FLOW ENFORCEMENT
AC-4(17).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system uniquely identifies source domains for information transfer;* *(ii) the information system uniquely authenticates source domains for information transfer;* *(iii) the information system uniquely identifies destination domains for information transfer;* *(iv) the information system uniquely authenticates destination domains for information transfer;* *(v) the information system binds security attributes to information to facilitate information flow policy enforcement;* *(vi) the information system tracks problems associated with the security attribute binding; and* *(vii) the information system tracks problems associated with the information transfer.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing information flow enforcement; procedures addressing source and destination domain identification and authentication; and information transfer error handling; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-5	**SEPARATION OF DUTIES**
AC-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;* *(ii) the organization documents separation of duties; and* *(iii) the organization implements separation of duties through assigned information system access authorizations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties]. **Test:** [*SELECT FROM:* Automated mechanisms implementing separation of duties policy].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-6	**LEAST PRIVILEGE**
AC-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(1)	**LEAST PRIVILEGE**
AC-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; and* *(ii) the organization explicitly authorizes access to the organization-defined security functions and security-relevant information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of security functions and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(2)	LEAST PRIVILEGE
AC-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access; and* *(ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions; and* *(iii) the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(3)	LEAST PRIVILEGE
AC-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the privileged commands to which network access is to be authorized only for compelling operational needs;* *(ii) the organization authorizes network access to organization-defined privileged commands only for compelling operational needs; and* *(iii) the organization documents the rationale for authorized network access to organization-defined privileged commands in the security plan for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing least privilege; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(4)	LEAST PRIVILEGE
AC-6(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides separate processing domains to enable finer-grained allocation of user privileges.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing least privilege; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(5)	LEAST PRIVILEGE
AC-6(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits authorization to super user accounts on the information system to designated system administration personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of system-generated super user accounts; list of system administration personnel; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

AC-6(6)	LEAST PRIVILEGE
AC-6(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits privileged access to the information system by non-organizational users.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing least privilege; list of system-generated privileged accounts; list of non-organizational users; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-7	**UNSUCCESSFUL LOGIN ATTEMPTS**
AC-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occur;* *(ii) the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;* *(iii) the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:* – *lock out the account/node for a specified time period;* – *lock out the account/note until released by an administrator; or* – *delay the next login prompt according to organization-defined delay algorithm;* *(iv) the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded; and* *(v) the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for unsuccessful login attempts].

AC-7(1)	UNSUCCESSFUL LOGIN ATTEMPTS
AC-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful login attempts is exceeded.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing unsuccessful login attempts; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for unsuccessful login attempts].

AC-7(2)	UNSUCCESSFUL LOGIN ATTEMPTS
AC-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the number of consecutive, unsuccessful login attempts allowed for accessing a mobile device before the information system purges information from the device; and* *(ii) the information system provides protection for mobile devices accessed via login by purging information from such devices after the organization-defined number of consecutive, unsuccessful login attempts to the device is exceeded.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing unsuccessful login attempts on mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for unsuccessful login attempts].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-8	**SYSTEM USE NOTIFICATION**
AC-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization approves the information system use notification message or banner to be displayed by the information system before granting access to the system;* *(ii) the information system displays the approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:* - *users are accessing a U.S. Government information system;* - *system usage may be monitored, recorded, and subject to audit;* - *unauthorized use of the system is prohibited and subject to criminal and civil penalties; and* - *use of the system indicates consent to monitoring and recording; and* *(iii) the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for system use notification].
AC-8.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;* *(ii) the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and* *(iii) the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for system use notification].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-9	**PREVIOUS LOGON (ACCESS) NOTIFICATION**
AC-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, upon successful user logon (access), displays to the user the date and time of the last logon (access).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing previous logon notification; information system configuration settings and associated documentation; information system notification messages; information system design documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for previous logon notification].

AC-9(1)	PREVIOUS LOGON (ACCESS) NOTIFICATION
AC-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, upon successful user logon/access, displays to the user the number of unsuccessful logon/access attempts since the last successful logon/access.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing previous logon notification; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for previous logon notification].

AC-9(2)	PREVIOUS LOGON (ACCESS) NOTIFICATION
AC-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period during which the number of successful logins/accesses and/or unsuccessful user login/access attempts occurs; and* *(ii) the information system notifies the user of the number of successful logins/accesses and/or unsuccessful login/access attempts that occur during the organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing previous logon notification; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for previous logon notification].

AC-9(3)	PREVIOUS LOGON (ACCESS) NOTIFICATION
AC-9(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for which security-related changes to the user's account occur; and* *(ii) the information system notifies the user of the organization-defined security-related changes to the user's account that occur during the organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing previous logon notification; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for previous logon notification].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-10	**CONCURRENT SESSION CONTROL**
AC-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum number of concurrent sessions to be allowed for each system account; and* *(ii) the information system limits the number of concurrent sessions for each system account to the organization-defined number of sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for concurrent session control].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-11	**SESSION LOCK**
AC-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of user inactivity after which the information system initiates a session lock;* *(ii) the information system initiates a session lock after the organization-defined time period of inactivity or upon receiving a request from a user;* *(iii) the information system retains the session lock until the user reestablishes access using established identification and authentication procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; security plan; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for session lock].

AC-11(1)	**SESSION LOCK**
AC-11(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing session lock; display screen with session lock activated; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system session lock mechanisms].

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-12	**SESSION TERMINATION** [Withdrawn: Incorporated into SC-10].
AC-12.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into SC-10]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into SC-10].

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-13	**SUPERVISION AND REVIEW — ACCESS CONTROL** [Withdrawn: Incorporated into AC-2 and AU-6].
AC-13.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into AC-2 and AU-6]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into AC-2 and AU-6].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-14	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**
AC-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies specific user actions that can be performed on the information system without identification or authentication; and* *(ii) the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records].

AC-14(1)	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**
AC-14(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records].

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-15	**AUTOMATED MARKING** [Withdrawn: Incorporated into MP-3].
AC-15.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into MP-3]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into MP-3].

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-16	**SECURITY ATTRIBUTES**
AC-16.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security attributes the information system binds to information:* *- in storage;* *- in process; and* *- in transmission; and* *(ii) the information system supports and maintains the binding of the organization-defined security attributes to information in storage, in process, and in transmission.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the binding of security attributes to information in storage, in process, and in transmission; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and maintaining the binding of security attributes to information in storage, in process, and in transmission].

AC-16(1)	**SECURITY ATTRIBUTES**
AC-16(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the dynamic reconfiguration of security attributes; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the dynamic reconfiguration of security attributes to information].

AC-16(2)	SECURITY ATTRIBUTES
AC-16(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies the entities authorized to change security attributes; and* *(ii) the information system allows authorized entities to change security attributes.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the change of security attributes; information system design documentation; information system configuration settings and associated documentation; list of entities authorized to change security attributes; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for changing security attributes]. **Test**: [*SELECT FROM:* Automated mechanisms allowing the change of security attributes].

AC-16(3)	SECURITY ATTRIBUTES
AC-16(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system maintains the binding of security attributes to information with sufficient assurance that the information-attribute association can be used as the basis for automated policy actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the binding of security attributes to information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms maintaining the binding of security attributes to information].

AC-16(4)	SECURITY ATTRIBUTES
AC-16(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies users authorized to associate security attributes with information; and* *(ii) the information system allows authorized users to associate security attributes with information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the association of security attributes to information; information system design documentation; information system configuration settings and associated documentation; list of users authorized to associate security attributes with information; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for associating security attributes with information]. **Test**: [*SELECT FROM:* Automated mechanisms allowing users to associate security attributes with information].

AC-16(5)	SECURITY ATTRIBUTES
AC-16(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the set of special dissemination, handling, or distribution instructions to be used for each object output from the information system;* *(ii) the organization defines standard naming conventions for the security attributes to be displayed in human-readable form on each object output from the system to system output devices; and* *(iii) the information system displays security attributes in human-readable form on each object output from the system to system output devices to identify the organization-defined set of special dissemination, handling, or distribution instructions using organization-defined human readable, standard naming conventions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing display of security attributes in human-readable form; special instructions for the dissemination, handling, or distribution of object output from the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* System output devices displaying security attributes in human-readable form on each object].

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-17	**REMOTE ACCESS**
AC-17.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization documents allowed methods of remote access to the information system;* *(ii) the organization establishes usage restrictions and implementation guidance for each allowed remote access method;* *(iii) the organization monitors for unauthorized remote access to the information system;* *(iv) the organization authorizes remote access to the information system prior to connection; and* *(v) the organization enforces requirements for remote connections to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with remote access authorization, monitoring, and control responsibilities]. **Test:** [*SELECT FROM:* Remote access methods for the information system].

AC-17(1)	**REMOTE ACCESS**
AC-17(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for remote access].

AC-17(2)	REMOTE ACCESS
AC-17(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses cryptography to protect the confidentiality and integrity of remote access sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing cryptographic protections for remote access].

AC-17(3)	REMOTE ACCESS
AC-17(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a limited number of managed access control points for remote access to the information system; and* *(ii) the information system routes all remote accesses through managed access control points.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for remote access].

AC-17(4)	REMOTE ACCESS
AC-17(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and* *(ii) the organization documents the rationale for such access in the security plan for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records].

AC-17(5)	REMOTE ACCESS
AC-17(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of monitoring for unauthorized remote connections to the information system;* *(ii) the organization monitors for unauthorized remote connections to the information system in accordance with the organization-defined frequency;* *(iii) the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and* *(iv) the organization takes organization-defined appropriate action(s) if an unauthorized connection is discovered.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for monitoring remote connections to the information system].

AC-17(6)	REMOTE ACCESS
AC-17(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for implementing or monitoring remote access to the information system; information system users with knowledge of information about remote access mechanisms].

AC-17(7)	REMOTE ACCESS
AC-17(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions and security-relevant information that can be accessed using remote sessions;* *(ii) the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;* *(iii) the organization employs organization-defined additional security measures for remote sessions used to access organization-defined security functions and security-relevant information; and* *(iv) the organization audits remote sessions for accessing organization-defined security functions and security-relevant information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the access control policy for remote access].

AC-17(8)	REMOTE ACCESS
AC-17(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the networking protocols within the information system deemed to be nonsecure; and* *(ii) the organization disables the organization-defined networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; security plan; list of networking protocols deemed to be non-secure; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms disabling networking protocols deemed to be non-secure].

FAMILY: ACCESS CONTROL

CLASS: TECHNICAL

ASSESSMENT PROCEDURE	
AC-18	**WIRELESS ACCESS**
AC-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for wireless access;* *(ii) the organization monitors for unauthorized wireless access to the information system;* *(iii) the organization authorizes wireless access to the information system prior to connection; and* *(iv) the organization enforces requirements for wireless connections to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system]. **Test:** [*SELECT FROM:* Wireless access usage and restrictions].

AC-18(1)	**WIRELESS ACCESS**
AC-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects wireless access to the system using authentication and encryption.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for wireless access to the information system].

AC-18(2)	WIRELESS ACCESS
AC-18(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of monitoring for unauthorized wireless connections to the information system, including scans for unauthorized wireless access points;* *(ii) the organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, in accordance with organization-defined frequency;* *(iii) the organization defines the appropriate action(s) to be taken if an unauthorized connection is discovered; and* *(iv) the organization takes appropriate action(s) if an unauthorized connection discovered.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel responsible for monitoring wireless connections to the information system]. **Test:** [*SELECT FROM:* Scanning procedures for detecting unauthorized wireless connections and access points].

AC-18(3)	WIRELESS ACCESS
AC-18(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization disables, when not intended for use, wireless networking capabilities internally embedded within the information system components prior to issuance and deployment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms controlling the disabling of wireless networking capabilities internally embedded within the information system components].

AC-18(4)	WIRELESS ACCESS
AC-18(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization does not allow users to independently configure wireless networking capabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms preventing independent configuration of wireless networking capabilities].

AC-18(5)	WIRELESS ACCESS
AC-18(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization confines wireless communications to organization-controlled boundaries.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing the access control policy for wireless access to the information system; Wireless connections and access points outside of organizational boundaries using scanning devices.].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-19	**ACCESS CONTROL FOR MOBILE DEVICES**
AC-19.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices;* *(ii) the organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;* *(iii) the organization monitors for unauthorized connections of mobile devices to organizational information systems;* *(iv) the organization enforces requirements for the connection of mobile devices to organizational information systems;* *(v) the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;* *(vi) the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;* *(vii) the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk; and* *(viii) the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel who use portable and mobile devices to access the information system]. **Test:** [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(1)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization restricts the use of writable, removable media in organizational information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel who use portable and mobile devices to access the information system]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(2)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits the use of personally owned, removable media in organizational information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(3)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access control policy for portable and mobile devices].

AC-19(4)	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s);* *(ii) the organization defines the security officials authorized to randomly review/inspect mobile devices and the information stored on those devices for classified information; and* *(iii) the organization enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:* - *connection of unclassified mobile devices to classified information systems is prohibited;* - *connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s);* - *use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and* - *mobile devices and the information stored on those devices are subject to random reviews/inspections by organization-defined security officials, and if classified information is found, the incident handling policy is enforced.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access control for portable and mobile devices; evidentiary documentation for random inspections of mobile devices; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel responsible for randomly reviewing/inspecting mobile devices; Organizational personnel using mobile devices in facilities containing information systems processing, storing, or transmitting classified information]. **Test**: [*SELECT FROM:* Test automated mechanisms prohibiting the use of internal or external modems or wireless interfaces with mobile devices].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-20	**USE OF EXTERNAL INFORMATION SYSTEMS**
AC-20.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies individuals authorized to:* - *access the information system from the external information systems; and* - *process, store, and/or transmit organization-controlled information using the external information systems; and* *(ii) the organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:* - *access the information system from the external information systems; and* - *process, store, and/or transmit organization-controlled information using the external information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems].

AC-20(1)	**USE OF EXTERNAL INFORMATION SYSTEMS**
AC-20(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:* – *can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or* – *has approved information system connection or processing agreements with the organizational entity hosting the external information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external information systems; security plan; information system connection or processing agreements; account management documents; other relevant documents or records].

AC-20(2)	USE OF EXTERNAL INFORMATION SYSTEMS
AC-20(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external information systems; security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-21	**USER-BASED COLLABORATION AND INFORMATION SHARING**
AC-21.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the circumstances where user discretion is required to facilitate information sharing;* *(ii) the organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the organization-defined circumstances;* *(iii) the organization defines the information sharing circumstances and automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions; and* *(iv) the organization employs organization-defined circumstances and automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); information system design documentation; information system configuration settings and associated documentation; list of users authorized to make information sharing/collaboration decisions; list of information sharing circumstances requiring user discretion; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel responsible for making information sharing/collaboration decisions]. **Test:** [*SELECT FROM:* Automated mechanisms or manual process implementing access authorizations supporting information sharing/user collaboration decisions].

AC-21(1)	USER-BASED COLLABORATION AND INFORMATION SHARING
AC-21(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); information system design documentation; information system configuration settings and associated documentation; system-generated list of users authorized to make information sharing/collaboration decisions; system-generated list of sharing partners and access authorizations; system-generated list of access restrictions regarding information to be shared; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing access authorizations supporting information sharing/user collaboration decisions].

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AC-22	**PUBLICLY ACCESSIBLE CONTENT**
AC-22.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible;* *(ii) the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;* *(iii) the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;* *(iv) the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information;* *(v) the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization-defined frequency; and* *(vi) the organization removes nonpublic information from the publicly accessible organizational information system, if discovered.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public Web sites; system audit logs; security awareness training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel responsible for managing publicly accessible information posted on organizational information systems].

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
AT-1	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**
AT-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents security awareness and training policy;* *(ii) the organization security awareness and training policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment; and* - *coordination among organizational entities, and compliance;* *(iii) the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;* *(iv) the organization develops and formally documents security awareness and training procedures;* *(v) the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls; and* *(vi) the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security awareness and training responsibilities].
AT-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of security awareness and training policy reviews/updates;* *(ii) the organization reviews/updates security awareness and training policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of security awareness and training procedure reviews/updates; and* *(iv) the organization reviews/updates security awareness and training procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security awareness and training responsibilities].

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
AT-2	**SECURITY AWARENESS**
AT-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;* *(ii) the organization defines the frequency of refresher security awareness training;* *(iii) the organization provides refresher security awareness training in accordance with the organization-defined frequency;* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel comprising the general information system user community].

AT-2(1)	**SECURITY AWARENESS**
AT-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes practical exercises in security awareness training that simulate actual cyber attacks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel that participate in security awareness training].

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
AT-3	**SECURITY TRAINING**
AT-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;* *(ii) the organization defines the frequency of refresher role-based security-related training;* *(iii) the organization provides refresher role-based security-related training in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant information system security responsibilities].

AT-3(1)	SECURITY TRAINING
AT-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides employees with initial training in the employment and operation of environment controls;* *(ii) the organization defines the frequency of refresher training in the employment and operation of environmental controls; and* *(iii) the organization provides refresher training in the employment and operation of environmental controls in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organization personnel with security training responsibilities; organizational personnel with significant information system security responsibilities].

AT-3(2)	SECURITY TRAINING
AT-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides employees with initial training in the employment and operation of physical security controls;* *(ii) the organization defines the frequency of refresher training in the employment and operation of physical security controls; and* *(iii) the organization provides refresher training in the employment and operation of physical security controls in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security training responsibilities; organizational personnel with significant information system security responsibilities].

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
AT-4	**SECURITY TRAINING RECORDS**
AT-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training;* *(ii) the organization defines the time period for retaining individual training records; and* *(iii) the organization retains individual training records in accordance with the organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security training record retention responsibilities].

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
AT-5	**CONTACTS WITH SECURITY GROUPS AND ASSOCIATION**
AT-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization establishes and institutionalizes contact with selected groups and associations within the security community:* – *to facilitate ongoing security education and training for organizational personnel;* – *to stay up to date with the latest recommended security practices, techniques, and technologies; and* – *to share current security-related information including threats, vulnerabilities, and incidents.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security responsibilities (e.g., individuals that have contacts with selected groups and associations within the security community)].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-1	**AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**
AU-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents audit and accountability policy;* *(ii) the organization audit and accountability policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;* *(iv) the organization develops and formally documents audit and accountability procedures;* *(v) the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls; and* *(vi) the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with audit and accountability responsibilities].
AU-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of audit and accountability policy reviews/updates;* *(ii) the organization reviews/updates audit and accountability policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of audit and accountability procedure reviews/updates; and* *(iv) the organization reviews/updates audit and accountability procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with audit and accountability responsibilities].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-2	**AUDITABLE EVENTS**
AU-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the list of events the information system must be capable of auditing based on a risk assessment and mission/business needs;* *(ii) the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;* *(iii) the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;* *(iv) the organization defines the subset of auditable events defined in (i) that are to be audited within the information system and the frequency of (or situation requiring) auditing for each identified event; and* *(v) the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (i) to be audited within the information system, and the frequency of (or situation requiring) auditing for each identified event .* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system auditing of organization-defined auditable events].

AU-2(1)	**AUDITABLE EVENTS** [Withdrawn: Incorporated into AU-12].
AU-2(1).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into AU-12]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into AU-12].

AU-2(2)	**AUDITABLE EVENTS** [Withdrawn: Incorporated into AU-12].
AU-2(2).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into AU-12]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into AU-12].

AU-2(3)	**AUDITABLE EVENTS**
AU-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of reviews and updates to the list of organization-defined auditable events; and* *(ii) the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities].

AU-2(4)	**AUDITABLE EVENTS**
AU-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes execution of privileged functions in the list of events to be audited by the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; information system configuration settings and associated documentation; list of organization-defined auditable events; list of privileged security functions; other relevant documents or records].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-3	**CONTENT OF AUDIT RECORDS**
AU-3.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system produces audit records that contain sufficient information to, at a minimum, establish:* – *what type of event occurred;* – *when (date and time) the event occurred;* – *where the event occurred;* – *the source of the event;* – *the outcome (success or failure) of the event; and* – *the identity of any user/subject associated with the event.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing information system auditing of auditable events].

AU-3(1)	CONTENT OF AUDIT RECORDS
AU-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject; and* *(ii) the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject].

AU-3(2)	CONTENT OF AUDIT RECORDS
AU-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the information system components for which the content of audit records generated is centrally managed; and* *(ii) the organization centrally manages the content of audit records generated by organization-defined information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing centralized management of audit record content].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-4	**AUDIT STORAGE CAPACITY**
AU-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization allocates audit record storage capacity; and* *(ii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Audit record storage capacity and related configuration settings].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-5	**RESPONSE TO AUDIT PROCESSING FAILURES**
AU-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines designated organizational officials to be alerted in the event of an audit processing failure;* *(ii) the information system alerts designated organizational officials in the event of an audit processing failure;* *(iii) the organization defines additional actions to be taken in the event of an audit processing failure; and* *(iv) the information system takes the additional organization-defined actions in the event of an audit processing failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing information system response to audit processing failures].

AU-5(1)	RESPONSE TO AUDIT PROCESSING FAILURES
AU-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided; and* *(ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing audit storage limit warnings].

AU-5(2)	RESPONSE TO AUDIT PROCESSING FAILURES
AU-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines audit failure events requiring real-time alerts; and* *(ii) the information system provides a real-time alert when organization-defined audit failure events occur.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing real time audit alerts when organization-defined audit failure events occur].

AU-5(3)	RESPONSE TO AUDIT PROCESSING FAILURES
AU-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic;* *(ii) the organization defines if the network traffic above configurable traffic volume thresholds are rejected or delayed; and* *(iii) the information system rejects or delays, as defined by the organization, network traffic generated above configurable traffic volume thresholds.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system capability implementing configurable traffic volume thresholds].

AU-5(4)	RESPONSE TO AUDIT PROCESSING FAILURES
AU-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system capability invoking system shutdown in the event of an audit failure].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING**
AU-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system audit record reviews and analyses;* *(ii) the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; and* *(iii) the organization reports findings of inappropriate/unusual activities, to designated organizational officials..* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Information system audit review, analysis, and reporting capability].
AU-6.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information , intelligence information, or other credible sources of information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].

AU-6(1)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; procedures for investigating and responding to suspicious activities; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities].

AU-6(2)	AUDIT REVIEW, ANALYSIS, AND REPORTING [Withdrawn: Incorporated into SI-4].
AU-6(2).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into SI-4]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into SI-4].

AU-6(3)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system audit records across different repositories; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].

AU-6(4)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system centralizes the review and analysis of audit records from multiple components within the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Information system capability for centralizing review and analysis of audit records from multiple information system components].

AU-6(5)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to enhance the ability to identify inappropriate or unusual activity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system capability for centralizing review and analysis of audit records from multiple information system components].

AU-6(6)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization correlates information from audit records with information obtained from monitoring physical access to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; security plan; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system capability for centralizing review and analysis of audit records from multiple information system components].

AU-6(7)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; security plan; other relevant documents or records].

AU-6(8)	AUDIT REVIEW, ANALYSIS, AND REPORTING [Withdrawn: Incorporated into SI-4].
AU-6(8).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into SI-4]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into SI-4].

AU-6(9)	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-6(9).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization performs full-text analysis of privileged functions executed in a physically dedicated information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-7	**AUDIT REDUCTION AND REPORT GENERATION**
AU-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides an audit reduction and report generation capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. **Test**: [*SELECT FROM:* Audit reduction and report generation capability].

AU-7(1)	**AUDIT REDUCTION AND REPORT GENERATION**
AU-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Audit reduction and report generation capability].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-8	**TIME STAMPS**
AU-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses internal system clocks to generate time stamps for audit records.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing time stamp generation].

AU-8(1)	**TIME STAMPS**
AU-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of internal clock synchronization for the information system;* *(ii) the organization defines the authoritative time source for internal clock synchronization; and* *(iii) the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing time stamp generation; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing internal information system clock synchronization].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-9	**PROTECTION OF AUDIT INFORMATION**
AU-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects audit information and audit tools from unauthorized:* – *access;* – *modification; and* – *deletion.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing audit information protection].

AU-9(1)	**PROTECTION OF AUDIT INFORMATION**
AU-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system produces audit records on hardware-enforced, write-once media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Media storage devices to hold audit records].

AU-9(2)	PROTECTION OF AUDIT INFORMATION
AU-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the system or media for storing back up audit records that is a different system or media than the system being audited;* *(ii) the organization defines the frequency of information system backups of audit records; and* *(iii) the information system backs up audit records, in accordance with the organization-defined frequency, onto organization-defined system or media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing protection of audit information; security plan; information system design documentation; information system configuration settings and associated documentation; system or media storing backups of information system audit records; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities].

AU-9(3)	PROTECTION OF AUDIT INFORMATION
AU-9(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities].

AU-9(4)	PROTECTION OF AUDIT INFORMATION
AU-9(4).1	**ASSESSMENT OBJECTIVE:** *Determine if :* *(i) the organization authorizes access to management of audit functionality to only a limited subset of privileged users; and* *(ii) the organization protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with auditing and accountability responsibilities].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-10	**NON-REPUDIATION**
AU-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects against an individual falsely denying having performed a particular action.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing non-repudiation capability].

AU-10(1)	**NON-REPUDIATION**
AU-10(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system associates the identity of the information producer with the information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing non-repudiation capability].

AU-10(2)	**NON-REPUDIATION**
AU-10(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system validates the binding of the information producer's identity to the information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing non-repudiation capability].

AU-10(3)	NON-REPUDIATION
AU-10(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing non-repudiation capability].

AU-10(4)	NON-REPUDIATION
AU-10(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing non-repudiation capability].

AU-10(5)	NON-REPUDIATION
AU-10(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines whether FIPS-validated or NSA-approved cryptography is employed to implement digital signatures; and* *(ii) the organization employs the organization-defined cryptography to implement digital signatures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Cryptographic mechanisms implementing digital signature capability within the information system].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-11	**AUDIT RECORD RETENTION**
AU-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the retention period for audit records;* *(ii) the retention period for audit records is consistent with the records retention policy; and* *(iii) the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit record retention responsibilities].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-12	**AUDIT GENERATION**
AU-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;* *(ii) the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;* *(iii) the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and* *(iv) the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system audit record generation responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing audit record generation capability].

AU-12(1)	**AUDIT GENERATION**
AU-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system produces a system-wide (logical or physical) audit trail of information system audit records;* *(ii) the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail;* *(iii) the information system compiles audit records from organization-defined information system components into the system-wide audit trail;* *(iv) the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail; and* *(v) the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing audit record generation capability].

AU-12(2)	AUDIT GENERATION
AU-12(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing audit record generation capability].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-13	**MONITORING FOR INFORMATION DISCLOSURE**
AU-13.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of monitoring open source information for evidence of unauthorized exfiltration or disclosure of organization information; and* *(ii) the organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing information disclosure monitoring; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure].

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
AU-14	**SESSION AUDIT**
AU-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system provides the capability to capture/record and log all content related to a user session; and* *(ii) the information system provides the capability to remotely view/hear all content related to an established user session in real time.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing user session auditing; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing user session auditing capability].

AU-14(1)	**SESSION AUDIT**
AU-14(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system initiates session audits at system start-up* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Audit and accountability policy; procedures addressing user session auditing; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing user session auditing capability].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-1	**SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES**
CA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents security assessment and authorization policy;* *(ii) the organization security assessment and authorization policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities;* *(iv) the organization develops and formally documents security assessment and authorization procedures;* *(v) the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and* *(vi) the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policies and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment and authorization responsibilities].
CA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of security assessment and authorization policy reviews/updates;* *(ii) the organization reviews/updates security assessment and authorization policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of security assessment and authorization procedure reviews/updates; and* *(iv) the organization reviews/updates security assessment and authorization procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policies and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment and authorization responsibilities].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-2	**SECURITY ASSESSMENTS**
CA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a security assessment plan for the information system; and* *(ii) the security assessment plan describes the scope of the assessment including:* - *security controls and control enhancements under assessment;* - *assessment procedures to be used to determine security control effectiveness; and* - *assessment environment, assessment team, and assessment roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security assessment plan; other relevant documents or records].
CA-2.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;* *(ii) the organization assesses the security controls in the information system at the organization-defined frequency;* *(iii) the organization produces a security assessment report that documents the results of the security control assessment; and* *(iv) the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

CA-2(1)	SECURITY ASSESSMENTS
CA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

CA-2(2)	SECURITY ASSESSMENTS
CA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *the forms of security testing to be included in security control assessments, selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing;* - *the frequency for conducting each form of security testing;* - *whether the security testing will be announced or unannounced; and* *(ii) the organization conducts security control assessments using organization-defined forms of testing in accordance with organization-defined frequency and assessment techniques established for each form of testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-3	**INFORMATION SYSTEM CONNECTIONS**
CA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);* *(ii) the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;* *(iii) the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and* *(iv) the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements].

CA-3(1)	INFORMATION SYSTEM CONNECTIONS
CA-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits the direct connection of an unclassified, national security system to an external network.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records].

CA-3(2)	INFORMATION SYSTEM CONNECTIONS
CA-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prohibits the direct connection of a classified, national security system to an external network.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection agreements; security plan; information system design documentation;; security assessment report; plan of action and milestones; other relevant documents or records].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-4	**SECURITY CERTIFICATION** [Withdrawn: Incorporated into CA-2].
CA-4.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into CA-2]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into CA-2].

CA-4(1)	**SECURITY CERTIFICATION** [Withdrawn: Incorporated into CA-2].
CA-4(1).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into CA-2]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into CA-2].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-5	**PLAN OF ACTION AND MILESTONES**
CA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a plan of action and milestones for the information system;* *(ii) the plan of action and milestones documents the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;* *(iii) the organization defines the frequency of plan of action and milestone updates; and* *(iv) the organization updates the plan of action and milestones at an organization-defined frequency with findings from:* - *security controls assessments;* - *security impact analyses; and* - *continuous monitoring activities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with plan of action and milestones development and implementation responsibilities].

CA-5(1)	PLAN OF ACTION AND MILESTONES
CA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:* – *accurate;* – *up to date; and* – *readily available.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with plan of action and milestones development and implementation responsibilities]. **Test:** [*SELECT FROM:* Automated mechanisms for developing, implementing and maintaining plan of action and milestones].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-6	**SECURITY AUTHORIZATION**
CA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assigns a senior-level executive or manager to the role of authorizing official for the information system;* *(ii) the authorizing official authorizes the information system for processing before commencing operations;* *(iii) the organization defines the frequency of security authorization updates; and* *(iv) the organization updates the security authorization in accordance with an organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security authorization responsibilities].

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
CA-7	**CONTINUOUS MONITORING**
CA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a continuous monitoring strategy and program;* *(ii) the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;* *(iii) the organization defines organizational officials to whom the security state of the information system should be reported; and* *(iv) the organization implements a continuous monitoring program that includes:* - *a configuration management process for the information system and its constituent components;* - *a determination of the security impact of changes to the information system and environment of operation;* - *ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and* - *reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities].

CA-7(1)	**CONTINUOUS MONITORING**
CA-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with continuous monitoring responsibilities].

CA-7(2)	CONTINUOUS MONITORING
CA-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;* - *the frequency for conducting each form of security testing;* - *whether the security testing will be announced or unannounced; and* *(ii) the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for each form of testing to ensure compliance with all vulnerability mitigation procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with continuous monitoring responsibilities].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-1	**CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**
CM-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents configuration management policy;* *(ii) the organization configuration management policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities;* *(iv) the organization develops and formally documents configuration management procedures;* *(v) the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; and* *(vi) the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management and control responsibilities].
CM-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of configuration management policy reviews/updates;* *(ii) the organization reviews/updates configuration management policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of configuration management procedure reviews/updates; and* *(iv) the organization reviews/updates configuration management procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration management and control responsibilities].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-2	**BASELINE CONFIGURATION**
CM-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents a baseline configuration of the information system and;* *(ii) the organization maintains, under configuration control, a current baseline configuration of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records].

CM-2(1)	BASELINE CONFIGURATION
CM-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* *- the frequency of reviews and updates to the baseline configuration of the information system; and;* *- the circumstances that require reviews and updates to the baseline configuration of the information system; and;* *(ii) the organization reviews and updates the baseline configuration of the information system:* *- in accordance with the organization-defined frequency;* *- when required due to organization-defined circumstances; and;* *- as an integral part of information system component installations and upgrades.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].

CM-2(2)	BASELINE CONFIGURATION
CM-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing baseline configuration maintenance].

CM-2(3)	BASELINE CONFIGURATION
CM-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization retains older versions of baseline configurations as deemed necessary to support rollback.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; historical copies of baseline configurations; other relevant documents or records].

CM-2(4)	BASELINE CONFIGURATION
CM-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and maintains a list of software programs not authorized to execute on the information system; and* *(ii) the organization employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software programs not authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records].

CM-2(5)	BASELINE CONFIGURATION
CM-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and maintains a list of software programs authorized to execute on the information system; and* *(ii) the organization employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; list of software authorized to execute on the information system; information system architecture and configuration documentation; security plan; other relevant documents or records].

CM-2(6)	BASELINE CONFIGURATION
CM-2(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing baseline configuration environments].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-3	**CONFIGURATION CHANGE CONTROL**
CM-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization determines the types of changes to the information system that are configuration controlled;* *(ii) the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses;* *(iii) the organization documents approved configuration-controlled changes to the system;* *(iv) the organization retains and reviews records of configuration-controlled changes to the system;* *(v) the organization audits activities associated with configuration-controlled changes to the system;* *(vi) the organization defines:* - *the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities;* - *the frequency with which the configuration change control element convenes; and/or;* - *configuration change conditions that prompt the configuration change control element to convene.* *(vii) the organization coordinates and provides oversight for configuration change control activities through the organization-defined configuration change control element that convenes at the organization-defined frequency and/or for any organization-defined configuration change conditions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].

CM-3(1)	CONFIGURATION CHANGE CONTROL
CM-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period after which approvals that have not been received for proposed changes to the information system are highlighted; and* *(ii) the organization employs automated mechanisms to:* - *document proposed changes to the information system;* - *notify designated approval authorities;* - *highlight approvals that have not been received by the organization-defined time period;* - *inhibit change until designated approvals are received; and* - *document completed changes to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing configuration change control].

CM-3(2)	CONFIGURATION CHANGE CONTROL
CM-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].

CM-3(3)	CONFIGURATION CHANGE CONTROL
CM-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to implement changes to the current information system baseline; and* *(ii) the organization deploys the updated baseline across the installed base.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing changes to the information system baseline].

CM-3(4)	CONFIGURATION CHANGE CONTROL
CM-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires an information security representative to be a member of the configuration change control element as defined by the organization in CM-3.1 (vi).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system configuration change control; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with configuration change control responsibilities].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-4	**SECURITY IMPACT ANALYSIS**
CM-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes].

CM-4(1)	**SECURITY IMPACT ANALYSIS**
CM-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization analyzes new software in a separate test environment before installation in an operational environment; and* *(ii) the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; information system test and operational environments; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes].

CM-4(2)	SECURITY IMPACT ANALYSIS
CM-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization, after the information system is changed, checks the security functions to verify that the functions are:* – *implemented correctly;* – *operating as intended; and* – *producing the desired outcome with regard to meeting the security requirements for the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-5	**ACCESS RESTRICTIONS FOR CHANGE**
CM-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities]. **Test:** [*SELECT FROM:* Change control process and associated restrictions for changes to the information system].

CM-5(1)	**ACCESS RESTRICTIONS FOR CHANGE**
CM-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing access restrictions for changes to the information system].

CM-5(2)	**ACCESS RESTRICTIONS FOR CHANGE**
CM-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for conducting audits of information system changes; and* *(ii) the organization conducts audits of information system changes in accordance with the organization-defined frequency and when indications so warrant to determine whether unauthorized changes have occurred.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records].

CM-5(3)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines critical software programs that the information system will prevent from being installed if such software programs are not signed with a recognized and approved certificate; and* *(ii) the information system prevents the installation of organization-defined critical software programs that are not signed with a certificate that is recognized and approved by the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; list of critical software programs to be prohibited from installation without an approved certificate; information system design documentation; information system architecture and configuration documentation; security plan; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate].

CM-5(4)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system components and system-level information requiring enforcement of a two-person rule for information system changes; and* *(ii) the organization enforces a two-person rule for changes to organization-defined information system components and system-level information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; security plan; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel responsible for enforcing a two-person rule for system changes].

CM-5(5)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment;* *(ii) the organization defines the frequency for reviews and reevaluations of information system developer/integrator privileges; and* *(iii) the organization reviews and reevaluates information system developer/integrator privileges in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; security plan; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities].

CM-5(6)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits privileges to change software resident within software libraries (including privileged programs).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records].

CM-5(7)	ACCESS RESTRICTIONS FOR CHANGE
CM-5(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines safeguards and countermeasures to be employed by the information system if security functions (or mechanisms) are changed inappropriately; and* *(ii) the information system automatically implements organization-defined safeguards and countermeasures if security functions (or mechanisms) are changed inappropriately.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system implementing safeguards and countermeasures for inappropriate changes to security functions].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-6	**CONFIGURATION SETTINGS**
CM-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;* *(ii) the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;* *(iii) the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;* *(iv) the organization implements the security configuration settings;* *(v) the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and* *(vi) the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security configuration responsibilities].

CM-6(1)	CONFIGURATION SETTINGS
CM-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the centralized management, application, and verification of configuration settings].

CM-6(2)	CONFIGURATION SETTINGS
CM-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines configuration settings that, if modified by unauthorized changes, initiate the automated mechanisms to be employed to respond to such changes; and* *(ii) the organization employs automated mechanisms to respond to unauthorized changes to organization-defined configuration settings.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing responses to unauthorized changes to configuration settings].

CM-6(3)	CONFIGURATION SETTINGS
CM-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability; and* *(ii) the organization ensures that such detected events are tracked, monitored, corrected, and available for historical purposes.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; procedures addressing incident response planning; information system design documentation; information system configuration settings and associated documentation; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities].

CM-6(4)	CONFIGURATION SETTINGS
CM-6(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security configuration responsibilities].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-7	**LEAST FUNCTIONALITY**
CM-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines for the information system prohibited or restricted:* - *functions;* - *ports;* - *protocols; and* - *services;* *(ii) the organization configures the information system to provide only essential capabilities; and* *(iii) the organization configures the information system to specifically prohibit or restrict the use of organization-defined:* - *functions;* - *ports;* - *protocols; and/or* - *services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system for disabling or restricting functions, ports, protocols, and services].

CM-7(1)	LEAST FUNCTIONALITY
CM-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system reviews to identify and eliminate unnecessary:* - *functions;* - *ports;* - *protocols; and/or* - *services; and* *(ii) the organization reviews the information system in accordance with organization-defined frequency to identify and eliminate unnecessary:* - *functions;* - *ports;* - *protocols; and/or* - *services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system].

CM-7(2)	LEAST FUNCTIONALITY
CM-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and maintains one or more of the following specifications to prevent software program execution on the information system:* - *a list of software programs authorized to execute on the information system;* - *a list of software programs not authorized to execute on the information system; and/or* - *rules authorizing the terms and conditions of software program usage on the information system; and* *(ii) the organization employs automated mechanisms to prevent software program execution on the information system in accordance with the organization-defined specifications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms preventing software program execution on the information system].

CM-7(3)	LEAST FUNCTIONALITY
CM-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines registration requirements for:* - *ports;* - *protocols; and* - *services; and* *(ii) the organization ensures compliance with organization-defined registration requirements for:* - *ports;* - *protocols; and* - *services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-8	**INFORMATION SYSTEM COMPONENT INVENTORY**
CM-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information deemed necessary to achieve effective property accountability; and* *(ii) the organization develops, documents, and maintains an inventory of information system components that:* - *accurately reflects the current information system;* - *is consistent with the authorization boundary of the information system;* - *is at the level of granularity deemed necessary for tracking and reporting;* - *includes organization-defined information deemed necessary to achieve effective property accountability; and* - *is available for review and audit by designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records].

CM-8(1)	**INFORMATION SYSTEM COMPONENT INVENTORY**
CM-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization updates the inventory of information system components as an integral part of component:* – *installations;* – *removals; and* – *information system updates.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system installation and inventory responsibilities].

CM-8(2)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing information system component inventory management].

CM-8(3)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of employing automated mechanisms to detect the addition of unauthorized components/devices into the information system;* *(ii) the organization employs automated mechanisms, in accordance with the organization-defined frequency, to detect the addition of unauthorized components/devices into the information system; and* *(iii) the organization disables network access by such components/devices or notifies designated organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system design documentation; information system inventory records; component installation records; change control records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms for detecting unauthorized components/devices on the information system].

CM-8(4)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes in property accountability information for information system components, a means for identifying by name, position, or role, individuals responsible for administering those components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records].

CM-8(5)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; component installation records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system inventory responsibilities; organizational personnel with responsibilities for defining information system components within the authorization boundary of the system].

CM-8(6)	INFORMATION SYSTEM COMPONENT INVENTORY
CM-8(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with inventory management and assessment responsibilities for information system components].

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CM-9	**CONFIGURATION MANAGEMENT PLAN**
CM-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops, documents, and implements a configuration management plan for the information system that:* – *addresses roles, responsibilities, and configuration management processes and procedures;* – *defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and* – *establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing configuration management planning; security plan; other relevant documents or records].

CM-9(1)	**CONFIGURATION MANAGEMENT PLAN**
CM-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing responsibilities for configuration management process development; security plan other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for configuration management process development].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-1	**CONTINGENCY PLANNING POLICY AND PROCEDURES**
CP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents contingency planning policy;* *(ii) the organization contingency planning policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;* *(iv) the organization develops and formally documents contingency planning procedures;* *(v) the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls; and* *(vi) the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning responsibilities].
CP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of contingency planning policy reviews/updates;* *(ii) the organization reviews/updates contingency planning policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of contingency planning procedure reviews/updates; and* *(iv) the organization reviews/updates contingency planning procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-2	**CONTINGENCY PLAN**
CP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a contingency plan for the information system that:* - *identifies essential missions and business functions and associated contingency requirements;* - *provides recovery objectives, restoration priorities, and metrics;* - *addresses contingency roles, responsibilities, assigned individuals with contact information;* - *addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and* - *addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and* - *is reviewed and approved by designated officials within the organization;* *(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan; and* *(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].
CP-2.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization coordinates contingency planning activities with incident handling activities;* *(ii) the organization defines the frequency of contingency plan reviews;* *(iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;* *(iv) the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing; and* *(v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements as identified in CP-2.1 (ii).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities].

CP-2(1)	CONTINGENCY PLAN
CP-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization coordinates the contingency plan development with other organizational elements responsible for related plans.* **Examine:** [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas].

CP-2(2)	CONTINGENCY PLAN
CP-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

CP-2(3)	CONTINGENCY PLAN
CP-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for planning the resumption of essential missions and business functions as a result of contingency plan activation; and* *(ii) the organization plans for the resumption of essential missions and business function within organization-defined time period of contingency plan activation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; business impact assessment; other related plans; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

CP-2(4)	CONTINGENCY PLAN
CP-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for planning the full resumption of affected missions and business functions as a result of contingency plan activation; and* *(ii) the organization plans for the full resumption of affected missions and business functions within organization-defined time period of contingency plan activation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; business impact assessment; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

CP-2(5)	CONTINGENCY PLAN
CP-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity; and* *(ii) the organization sustains operational continuity until full information system restoration at primary processing and/or storage sites.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; business impact assessment; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

CP-2(6)	CONTINGENCY PLAN
CP-2(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity; and* *(ii) the organization sustains operational continuity through restoration to primary processing and/or storage sites.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; alternate processing site agreements; alternate storage site agreements; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities].

FAMILY: CONTINGENCY PLANNING

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
CP-3	**CONTINGENCY TRAINING**
CP-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;* *(ii) the organization defines the frequency of refresher contingency training; and* *(iii) the organization provides refresher training in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and training responsibilities].

CP-3(1)	CONTINGENCY TRAINING
CP-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization incorporates simulated events into contingency training; and* *(ii) the incorporation of simulated events into contingency training facilitates effective response by personnel in crisis situations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and training responsibilities].

CP-3(2)	CONTINGENCY TRAINING
CP-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms that provide a more thorough and realistic contingency training environment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing contingency training; automated mechanisms supporting contingency training; contingency training curriculum; contingency training material; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and training responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-4	**CONTINGENCY PLAN TESTING AND EXERCISES**
CP-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the contingency plan tests and/or exercises to be conducted;* *(ii) the organization defines the frequency of contingency plan tests and/or exercises;* *(iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; and* *(iv) the organization reviews the contingency plan test/exercise results and takes corrective actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises].

CP-4(1)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and testing responsibilities; organizational personnel with responsibilities for related plans].

CP-4(2)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts contingency plan testing/exercises at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records].

CP-4(3)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and/or exercise documentation; other relevant documents or records].

CP-4(4)	CONTINGENCY PLAN TESTING AND EXERCISES
CP-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency plan testing and/or exercise responsibilities].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-5	**CONTINGENCY PLAN UPDATE** [Withdrawn: Incorporated into CP-2].
CP-5.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into CP-2]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into CP-2].
CP-5.2	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into CP-2]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into CP-2].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-6	**ALTERNATE STORAGE SITE**
CP-6.1	**ASSESSMENT OBJECTIVE:** *Determine if :* *(i) the organization establishes an alternate storage site; and* *(ii) the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records].

CP-6(1)	ALTERNATE STORAGE SITE
CP-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies the primary storage site hazards; and* *(ii) the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records].

CP-6(2)	ALTERNATE STORAGE SITE
CP-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate storage site is configured to facilitate recovery operations in accordance with recovery time objectives and recovery point objectives.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; other relevant documents or records].

CP-6(3)	ALTERNATE STORAGE SITE
CP-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and* *(ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; mitigation actions for accessibility problems to the alternate storage site; other relevant documents or records].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-7	**ALTERNATE PROCESSING SITE**
CP-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes an alternate processing site;* *(ii) the organization defines the time period for achieving the recovery time objectives within which processing must be resumed at the alternate processing site;* *(iii) the organization includes necessary alternate processing site agreements to permit the resumption of information system operations for essential missions and business functions within organization-defined time period; and* *(iv) the equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; other relevant documents or records].

CP-7(1)	ALTERNATE PROCESSING SITE
CP-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the contingency plan identifies the primary processing site hazards; and* *(ii) the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records].

CP-7(2)	ALTERNATE PROCESSING SITE
CP-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and* *(ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records].

CP-7(3)	ALTERNATE PROCESSING SITE
CP-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records].

CP-7(4)	ALTERNATE PROCESSING SITE
CP-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate processing site is configured so that it is ready to be used as the operational site to support essential missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system at the alternate processing site].

CP-7(5)	ALTERNATE PROCESSING SITE
CP-7(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the alternate processing site provides information security measures equivalent to that of the primary site.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-8	**TELECOMMUNICATIONS SERVICES**
CP-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes alternate telecommunications services to support the information system;* *(ii) the organization defines in the time period within which resumption of information system operations must take place; and* *(iii) the organization establishes necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; other relevant documents or records].

CP-8(1)	TELECOMMUNICATIONS SERVICES
CP-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements; and* *(ii) the organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; other relevant documents or records].

CP-8(2)	TELECOMMUNICATIONS SERVICES
CP-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers].

CP-8(3)	TELECOMMUNICATIONS SERVICES
CP-8(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies the primary provider's telecommunications service hazards; and* *(ii) the alternate telecommunications service providers are separated from the primary telecommunications service providers so as not to be susceptible to the same hazards.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; alternate telecommunications service provider's site; primary telecommunications service provider's site; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers].

CP-8(4)	TELECOMMUNICATIONS SERVICES
CP-8(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires primary and alternate telecommunications service providers to have contingency plans.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers].

FTC-0002525

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-9	**INFORMATION SYSTEM BACKUP**
CP-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives;* *(ii) the organization defines the frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives;* *(iii) the organization defines the frequency of conducting information system documentation backups (including security-related information) to support recovery time objectives and recovery point objectives;* *(iv) the organization backs up user-level information in accordance with the organization-defined frequency;* *(v) the organization backs up system-level information in accordance with the organization-defined frequency; and* *(vi) the organization backs up information system documentation in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system backup responsibilities].
CP-9.2	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects the confidentiality and integrity of backup information at the storage location.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system backup responsibilities].

CP-9(1)	INFORMATION SYSTEM BACKUP
CP-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of information system backup testing; and* *(ii) the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; information system backup test results; backup storage location(s); other relevant documents or records].

CP-9(2)	INFORMATION SYSTEM BACKUP
CP-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records].

CP-9(3)	INFORMATION SYSTEM BACKUP
CP-9(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization stores backup copies of operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information system backup responsibilities].

CP-9(4)	INFORMATION SYSTEM BACKUP [Withdrawn: Incorporated into CP-9].
CP-9(4).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into CP-9]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into CP-9].

CP-9(5)	INFORMATION SYSTEM BACKUP
CP-9(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period and rate of transferring information system backup information to the alternate storage site to support recovery time objectives and recovery point objectives; and* *(ii) the organization transfers information system backup information to the alternate storage site in accordance with the organization-defined frequency and transfer rate.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; information system backup test results; alternate site service agreements; backup storage location(s); other relevant documents or records].

CP-9(6)	INFORMATION SYSTEM BACKUP
CP-9(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization maintains a redundant, secondary backup system that is not collocated with the primary backup system for the information system; and* *(ii) the redundant, secondary backup system can be activated to accomplish information system backups without causing loss of information or disruption to the operation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan test results; contingency plan testing and/or exercise documentation; secondary backup storage location(s); redundant secondary system for information system backups; other relevant documents or records].

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
CP-10	**INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**
CP-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms and/or manual procedures for implementing information system recovery and reconstitution operations].

CP-10(1)	**INFORMATION SYSTEM RECOVERY AND RECONSTITUTION** [Withdrawn: Incorporated into CP-4(4)].
CP-10(1).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into CP-4(4)]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into CP-4(4)].

CP-10(2)	**INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**
CP-10(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements transaction recovery for systems that are transaction-based.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; contingency plan test results; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing transaction recovery capability].

CP-10(3)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines in the security plan, explicitly or by reference, the circumstances that can inhibit recovery and reconstitution of the information system to a known state; and* *(ii) the organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution of the information system to a known state.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities].

CP-10(4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time-periods within which information system components must be reimaged from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components; and* *(ii) the organization provides the capability to reimage information system components, within organization-defined time-periods, from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities].

CP-10(5)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the type of failover capability for the information system (including whether the capability will be real-time or near real-time); and* *(ii) the organization provides the organization-defined failover capability for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities]. **Test**: [*SELECT FROM:* Failover capability for the information system].

CP-10(6)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects backup and restoration hardware, firmware, and software.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; location(s) of backup and restoration hardware, firmware, and software; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system recovery and reconstitution responsibilities].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-1	**IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**
IA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents identification and authentication policy;* *(ii) the organization identification and authentication policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities;* *(iv) the organization develops and formally documents identification and authentication procedures;* *(v) the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls; and* *(vi) the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with identification and authentication responsibilities].
IA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of identification and authentication policy reviews/updates;* *(ii) the organization reviews/updates identification and authentication policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of identification and authentication procedure reviews/updates;* *(iv) the organization reviews/updates identification and authentication procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with identification and authentication responsibilities].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-2	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**
IA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(1)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for network access to privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(2)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for network access to non-privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(3)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for local access to privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(4)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for local access to non-privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(5)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and* *(ii) the organization requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(6)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(7)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(8)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and* *(ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

IA-2(9)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-2(9).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the replay-resistant authentication mechanisms to be used for network access to non-privileged accounts; and* *(ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-3	**DEVICE IDENTIFICATION AND AUTHENTICATION**
IA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system; and* *(ii) the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing device identification and authentication].

IA-3(1)	DEVICE IDENTIFICATION AND AUTHENTICATION
IA-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system authenticates devices before establishing remote network connections using bi-directional authentication between devices that is cryptographically based; and* *(ii) the information system authenticates devices before establishing wireless network connections using bi-directional authentication between devices that is cryptographically based.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing device identification and authentication].

IA-3(2)	DEVICE IDENTIFICATION AND AUTHENTICATION
IA-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing device identification and authentication].

IA-3(3)	DEVICE IDENTIFICATION AND AUTHENTICATION
IA-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to DHCP-enabled devices; and* *(ii) the organization audits DHCP lease information (including IP addresses) when assigned to a DHCP-enabled devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; information system configuration settings and associated documentation; DHCP lease information; device connection reports; other relevant documents or records].

FTC-0002538

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-4	**IDENTIFIER MANAGEMENT**
IA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for preventing reuse of user or device identifiers;* *(ii) the organization defines the time period of inactivity after which a user identifier is to be disabled; and* *(iii) the organization manages information system identifiers for users and devices by:* - *receiving authorization from a designated organizational official to assign a user or device identifier;* - *selecting an identifier that uniquely identifies an individual or device;* - *assigning the user identifier to the intended party or the device identifier to the intended device;* - *preventing reuse of user or device identifiers for the organization-defined time period; and* - *disabling the user identifier after the organization-defined time period of inactivity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with identifier management responsibilities].

IA-4(1)	**IDENTIFIER MANAGEMENT**
IA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if organization prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

IA-4(2)	IDENTIFIER MANAGEMENT
IA-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires that registration to receive a user ID and password include authorization by a supervisor; and* *(ii) the organization requires that registration to receive a user ID and password be done in person before a designated registration authority.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; user ID and password registration documentation; ID and password authorization records; registration authority records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with identifier management responsibilities].

IA-4(3)	IDENTIFIER MANAGEMENT
IA-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; identifier certification documentation; organizational personnel biometrics records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with identifier management responsibilities].

IA-4(4)	IDENTIFIER MANAGEMENT
IA-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the characteristic to be used to identify user status; and* *(ii) the organization manages user identifiers by uniquely identifying the user with the organization-defined characteristic identifying user status.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; list of characteristics identifying user status; other relevant documents or records].

IA-4(5)	IDENTIFIER MANAGEMENT
IA-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system dynamically manages:* – *identifiers;* – *attributes; and* – *associated access authorizations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing identifier management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing identifier management functions].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-5	**AUTHENTICATOR MANAGEMENT**
IA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period (by authenticator type) for changing/refreshing authenticators; and* *(ii) the organization manages information system authenticators for users and devices by:* - *verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;* - *establishing initial authenticator content for authenticators defined by the organization;* - *ensuring that authenticators have sufficient strength of mechanism for their intended use;* - *establishing and implementing administrative procedures for initial authenticator distribution;* - *establishing and implementing administrative procedures for lost/compromised or damaged authenticators;* - *establishing and implementing administrative procedures for revoking authenticators;* - *changing default content of authenticators upon information system installation;* - *establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);* - *changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;* - *protecting authenticator content from unauthorized disclosure and modification; and* - *requiring users to take, and having devices implement, specific measures to safeguard authenticators.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for determining initial authenticator content]. **Test**: [*SELECT FROM:* Automated mechanisms implementing authenticator management functions].

IA-5(1)	AUTHENTICATOR MANAGEMENT
IA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type;* *(ii) the organization defines the minimum number of characters that must be changed when new passwords are created;* *(iii) the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters;* *(iv) the organization defines the number of generations for which password reuse is prohibited; and* *(v) the information system, for password-based authentication:* - *enforces the minimum password complexity standards that meet the organization-defined requirements;* - *enforces the organization-defined minimum number of characters that must be changed when new passwords are created;* - *encrypts passwords in storage and in transmission;* - *enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and* - *prohibits password reuse for the organization-defined number of generations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing authenticator management functions].

IA-5(2)	AUTHENTICATOR MANAGEMENT
IA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system, for PKI-based authentication:* – *validates certificates by constructing a certification path with status information to an accepted trust anchor;* – *enforces authorized access to the corresponding private key; and* – *maps the authenticated identity to the user account.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for PKI-based authentication management]. **Test**: [*SELECT FROM:* Automated mechanisms implementing PKI-based authenticator management functions].

IA-5(3)	AUTHENTICATOR MANAGEMENT
IA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and* *(ii) the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with authenticator management responsibilities].

IA-5(4)	AUTHENTICATOR MANAGEMENT
IA-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; automated tools for testing authenticators; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with authenticator management responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms for authenticator strength].

IA-5(5)	AUTHENTICATOR MANAGEMENT
IA-5(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for information system procurements or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with authenticator management responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities].

IA-5(6)	AUTHENTICATOR MANAGEMENT
IA-5(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects authenticators commensurate with the classification or sensitivity of the information accessed.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; information classification or sensitivity documentation; security categorization documentation for the information system; security assessments of authenticator protections; risk assessment results; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections].

IA-5(7)	AUTHENTICATOR MANAGEMENT
IA-5(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; other relevant documents or records].

IA-5(8)	AUTHENTICATOR MANAGEMENT
IA-5(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines measures taken to manage the risk of compromise due to individuals having accounts on multiple information systems; and* *(ii) the organization takes organization-defined measures to manage the risk of compromise due to individuals having accounts on multiple information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator management; security plan; list of individuals having accounts on multiple information systems; list of measures intended to manage risk of compromise due to individuals having accounts on multiple information systems ; other relevant documents or records].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-6	**AUTHENTICATOR FEEDBACK**
IA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing authenticator feedback].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-7	**CRYPTOGRAPHIC MODULE AUTHENTICATION**
IA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Identification and authentication policy; procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing cryptographic module authentication].

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
IA-8	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**
IA-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing identification and authentication capability for the information system].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-1	**INCIDENT RESPONSE POLICY AND PROCEDURES**
IR-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents incident response policy;* *(ii) the organization incident response policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;* *(iv) the organization develops and formally documents incident response procedures;* *(v) the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls; and* *(vi) the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response responsibilities].
IR-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of incident response policy reviews/updates;* *(ii) the organization reviews/updates incident response policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of incident response procedure reviews/updates; and* *(iv) the organization reviews/updates incident response procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response responsibilities].

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
IR-2	**INCIDENT RESPONSE TRAINING**
IR-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies personnel with incident response roles and responsibilities with respect to the information system;* *(ii) the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;* *(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;* *(iv) the organization defines the frequency of refresher incident response training; and* *(v) the organization provides refresher incident response training in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response training and operational responsibilities].

IR-2(1)	**INCIDENT RESPONSE TRAINING**
IR-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response training; incident response training material; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response training and operational responsibilities].

IR-2(2)	**INCIDENT RESPONSE TRAINING**
IR-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response training; incident response training material; automated mechanisms supporting incident response training; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response training and operational responsibilities].

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
IR-3	**INCIDENT RESPONSE TESTING AND EXERCISES**
IR-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines incident response tests/exercises;* *(ii) the organization defines the frequency of incident response tests/exercises;* *(iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;* *(iv) the organization documents the results of incident response tests/exercises; and* *(v) the organization determines the effectiveness of the incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing material; incident response test results; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident response testing responsibilities].

IR-3(1)	INCIDENT RESPONSE TESTING AND EXERCISES
IR-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident response testing responsibilities].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-4	**INCIDENT HANDLING**
IR-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization implements an incident handling capability for security incidents that includes:* - *preparation;* - *detection and analysis;* - *containment;* - *eradication; and* - *recovery;* *(ii) the organization coordinates incident handling activities with contingency planning activities; and* *(iii) the organization incorporates lessons learned from ongoing incident handling activities into:* - *incident response procedures;* - *training; and* - *testing/exercises; and* *(iv) the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities]. **Test**: [*SELECT FROM:* Incident handling capability for the organization].

IR-4(1)	**INCIDENT HANDLING**
IR-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to support the incident handling process.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities].

IR-4(2)	INCIDENT HANDLING
IR-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes dynamic reconfiguration of the information system as part of the incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities].

IR-4(3)	INCIDENT HANDLING
IR-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies classes of incidents; and* *(ii) the organization defines the appropriate actions to take in response to each class of incidents to ensure continuation of organizational missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities].

IR-4(4)	INCIDENT HANDLING
IR-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; incident response plan; automated mechanisms supporting incident handling; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities].

IR-4(5)	INCIDENT HANDLING
IR-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a list of security violations that, if detected, initiate a configurable capability to automatically disable the information system; and* *(ii) the organization implements a configurable capability to automatically disable the information system if any of the organization-defined security violations are detected.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident handling responsibilities].

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
IR-5	**INCIDENT MONITORING**
IR-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tracks and documents information system security incidents.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident monitoring responsibilities]. **Test**: [*SELECT FROM:* Incident monitoring capability for the organization].

IR-5(1)	**INCIDENT MONITORING**
IR-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to assist in the tracking of security incidents;* *(ii) the organization employs automated mechanisms to assist in the collection of security incident information; and* *(iii) the organization employs automated mechanisms to assist in the analysis of security incident information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident monitoring responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-6	**INCIDENT REPORTING**
IR-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines in the time period required to report suspected security incidents to the organizational incident response capability;* *(ii) the organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period; and* *(iii) the organization reports security incident information to designated authorities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident reporting responsibilities].

IR-6(1)	INCIDENT REPORTING
IR-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident reporting responsibilities].

IR-6(2)	INCIDENT REPORTING
IR-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident reporting responsibilities].

FAMILY: INCIDENT RESPONSE

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
IR-7	**INCIDENT RESPONSE ASSISTANCE**
IR-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and* *(ii) the incident response support resource is an integral part of the organization's incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident response assistance and support responsibilities].

IR-7(1)	**INCIDENT RESPONSE ASSISTANCE**
IR-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident response support and assistance responsibilities; organizational personnel that require incident response support and assistance].

IR-7(2)	**INCIDENT RESPONSE ASSISTANCE**
IR-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and* *(ii) the organization identifies organizational incident response team members to the external providers.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; incident response plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with incident response support and assistance responsibilities; external providers of information system protection capability].

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
IR-8	**INCIDENT RESPONSE PLAN**
IR-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops an incident response plan that:* – *provides the organization with a roadmap for implementing its incident response capability;* – *describes the structure and organization of the incident response capability;* – *provides a high-level approach for how the incident response capability fits into the overall organization;* – *meets the unique requirements of the organization, which relate to mission, size, structure, and functions;* – *defines reportable incidents;* – *provides metrics for measuring the incident response capability within the organization;* – *defines the resources and management support needed to effectively maintain and mature an incident response capability; and* – *is reviewed and approved by designated officials within the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response planning responsibilities].
IR-8.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;* *(ii) the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;* *(iii) the organization defines, in the incident response plan, the frequency to review the plan;* *(iv) the organization reviews the incident response plan in accordance with the organization-defined frequency;* *(v) the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and* *(vi) the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with incident response planning responsibilities].

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-1	**SYSTEM MAINTENANCE POLICY AND PROCEDURES**
MA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system maintenance policy;* *(ii) the organization system maintenance policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;* *(iv) the organization develops and formally documents system maintenance procedures;* *(v) the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls; and* *(vi) the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].
MA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system maintenance policy reviews/updates;* *(ii) the organization reviews/updates system maintenance policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of system maintenance procedure reviews/updates;* *(iv) the organization reviews/updates system maintenance procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MA-2	**CONTROLLED MAINTENANCE**
MA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;* *(ii) the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;* *(iii) the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;* *(iv) the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and* *(v) the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-2(1)	**CONTROLLED MAINTENANCE**
MA-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains maintenance records for the information system that include:* – *date and time of maintenance;* – *name of the individual performing the maintenance;* – *name of escort, if necessary;* – *a description of the maintenance performed; and* – *a list of equipment removed or replaced (including identification numbers, if applicable).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records].

MA-2(2)	CONTROLLED MAINTENANCE
MA-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required; and* *(ii) the organization employs automated mechanisms to produce up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process and complete.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; procedures addressing controlled maintenance for the information system; automated mechanisms supporting information system maintenance activities; information system configuration settings and associated documentation; maintenance records; other relevant documents or records].

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-3	**MAINTENANCE TOOLS**
MA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization approves, controls, and monitors the use of information system maintenance tools; and* *(ii) the organization maintains information system maintenance tools on an ongoing basis.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records].

MA-3(1)	**MAINTENANCE TOOLS**
MA-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-3(2)	**MAINTENANCE TOOLS**
MA-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization checks all media containing diagnostic and test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities]. **Test:** [*SELECT FROM:* Media checking process for malicious code detection].

MA-3(3)	MAINTENANCE TOOLS
MA-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prevents the unauthorized removal of maintenance equipment by one of the following:* – *verifying that there is no organizational information contained on the equipment;* – *sanitizing or destroying the equipment;* – *retaining the equipment within the facility; or* – *obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-3(4)	MAINTENANCE TOOLS
MA-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; automated mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting information system maintenance activities].

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-4	**NON-LOCAL MAINTENANCE**
MA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization authorizes, monitors, and controls non-local maintenance and diagnostic activities;* *(ii) the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;* *(iii) the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;* *(iv) the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;* *(v) the organization maintains records for non-local maintenance and diagnostic activities; and* *(vi) the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-4(1)	NON-LOCAL MAINTENANCE
MA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization audits non-local maintenance and diagnostic sessions; and* *(ii) designated organizational personnel review the maintenance records of the sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; maintenance records; audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-4(2)	NON-LOCAL MAINTENANCE
MA-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization documents the installation and use of non-local maintenance and diagnostic connections in the security plan for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records].

MA-4(3)	NON-LOCAL MAINTENANCE
MA-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires and ensures non-local maintenance and diagnostic services are performed from an information system that implements a level of security at least as high as the level of security implemented on the information system being serviced; or* *(ii) the organization removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities; and* *(iii) the organization after the removed component service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities; information system maintenance provider].

MA-4(4)	NON-LOCAL MAINTENANCE
MA-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user; and* *(ii) the organization protects non-local maintenance sessions by separating the maintenance session from other network sessions with the information system by:* - *either physically separated communications paths; or* - *logically separated communications paths based upon encryption.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-4(5)	NON-LOCAL MAINTENANCE
MA-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the organizational personnel to be notified when non-local maintenance is planned;* *(ii) the organization requires that maintenance personnel notify organization-defined personnel when non-local maintenance is planned (i.e., date/time); and* *(iii) the organization requires that a designated organizational official with specific information security/information system knowledge approves the non-local maintenance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; maintenance records; audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-4(6)	NON-LOCAL MAINTENANCE
MA-4(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; cryptographic mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Cryptographic mechanisms supporting information system maintenance activities].

MA-4(7)	NON-LOCAL MAINTENANCE
MA-4(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing non-local maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; audit records; other relevant documents or records].

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MA-5	**MAINTENANCE PERSONNEL**
MA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes a process for maintenance personnel authorization;* *(ii) the organization maintains a current list of authorized maintenance organizations or personnel; and* *(iii) personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

MA-5(1)	MAINTENANCE PERSONNEL
MA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:* – *maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;* – *prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances, or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and* – *in the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system maintenance policy; procedures addressing maintenance personnel; information system media protection policy; physical and environmental protection policy; security plan; list of maintenance personnel requiring escort/supervision; maintenance records; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities].

MA-5(2)	MAINTENANCE PERSONNEL
MA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are cleared for the highest level of information on the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing maintenance personnel; maintenance records; access control records; access authorizations; access credentials; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities; organizational personnel with personnel security responsibilities].

MA-5(3)	MAINTENANCE PERSONNEL
MA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if personnel performing maintenance and diagnostic activities on the information system processing, storing, or transmitting classified information are U.S. citizens.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing maintenance personnel; maintenance records; access control records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities].

MA-5(4)	MAINTENANCE PERSONNEL
MA-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) cleared foreign nationals are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and* *(ii) the organization documents in a Memorandum of Agreement the approvals, consents, and detailed operational conditions under which foreign nationals are allowed to conduct maintenance and diagnostic activities on an information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing maintenance personnel; information system media protection policy; access control policy and procedures; physical and environmental protection policy and procedures; memorandum of agreement; maintenance records; access control records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities].

FAMILY: MAINTENANCE

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MA-6	**TIMELY MAINTENANCE**
MA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines security-critical information system components and/or key information technology components for which it will obtain maintenance support and/or spare parts;* *(ii) the organization defines the time period within which support and/or spare parts must be obtained after a failure; and* *(iii) the organization obtains maintenance support and/or spare parts for the organization-defined list of security-critical information system components and/or key information technology components within the organization-defined time period of failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; security plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system maintenance responsibilities].

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
MP-1	**MEDIA PROTECTION POLICY AND PROCEDURES**
MP-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents media protection policy;* *(ii) the organization media protection policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;* *(iv) the organization develops and formally documents media protection procedures;* *(v) the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls; and* *(vi) the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Media protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].
MP-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of media protection policy reviews/updates;* *(ii) the organization reviews/updates media protection policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of media protection procedure reviews/updates;* *(iv) the organization reviews/updates media protection procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Media protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MP-2	**MEDIA ACCESS**
MP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *digital and non-digital media requiring restricted access;* - *individuals authorized to access the media;* - *security measures taken to restrict access; and* *(ii) the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].

MP-2(1)	MEDIA ACCESS
MP-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automated mechanisms to restrict access to media storage areas; and* *(ii) the organization employs automated mechanisms to audit access attempts and access granted to media storage areas.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access restrictions to media storage areas].

MP-2(2)	MEDIA ACCESS
MP-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; other relevant documents or records]. **Test**: [*SELECT FROM:* Cryptographic mechanisms protecting and restricting access to information system information on portable digital media].

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MP-3	**MEDIA MARKING**
MP-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines removable media types and information system output that require marking;* *(ii) the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;* *(iii) the organization defines:* - *removable media types and information system output exempt from marking;* - *controlled areas designated for retaining removable media and information output exempt from marking; and* *(iv) removable media and information system output exempt from marking remain within designated controlled areas.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and information system output; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system media protection and marking responsibilities].

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MP-4	**MEDIA STORAGE**
MP-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *types of digital and non-digital media physically controlled and securely stored within designated controlled areas;* - *controlled areas designated to physically control and securely store the media;* - *security measures to physically control and securely store the media within designated controlled areas;* *(ii) the organization physically controls and securely stores organization-defined information system media within organization-defined controlled areas using organization-defined security measures; and* *(iii) the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection and storage responsibilities].

MP-4(1)	**MEDIA STORAGE**
MP-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs cryptographic mechanisms to protect information in storage.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Cryptographic mechanisms protecting information in storage].

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MP-5	**MEDIA TRANSPORT**
MP-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *types of digital and non-digital media protected and controlled during transport outside of controlled areas;* - *security measures (e.g., locked container, encryption) for such media transported outside of controlled areas;* *(ii) the organization protects and controls organization-defined information system media during transport outside of controlled areas using organization-defined security measures;* *(iii) the organization maintains accountability for information system media during transport outside of controlled areas;* *(iv) the organization identifies personnel authorized to transport information system media outside of controlled areas; and* *(v) the organization restricts the activities associated with transport of information system media to authorized personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media transport responsibilities].

MP-5(1)	**MEDIA TRANSPORT** [Withdrawn: Incorporated into MP-5].
MP-5(1).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into MP-5]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into MP-5].

MP-5(2)	MEDIA TRANSPORT
MP-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization documents activities associated with the transport of information system media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; information system media transport records; audit records; other relevant documents or records].

MP-5(3)	MEDIA TRANSPORT
MP-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an identified custodian throughout the transport of information system media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media transport responsibilities].

MP-5(4)	MEDIA TRANSPORT
MP-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media transport; information system media transport records; audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Cryptographic mechanisms protecting information during transportation outside controlled areas].

FAMILY: MEDIA PROTECTION

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
MP-6	**MEDIA SANITIZATION**
MP-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization sanitizes information system media both digital and non-digital prior to:* - *disposal;* - *release out of organizational control; or* - *release for reuse; and* *(ii) the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(1)	MEDIA SANITIZATION
MP-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(2)	MEDIA SANITIZATION
MP-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for testing sanitization equipment and procedures to verify correct performance; and* *(ii) the organization tests sanitization equipment and procedures to verify correct performance in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(3)	MEDIA SANITIZATION
MP-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines circumstances requiring sanitization of portable, removable storage devices prior to connecting such devices to the information system; and* *(ii) the organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under organization-defined circumstances.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(4)	MEDIA SANITIZATION
MP-6(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization sanitizes information system media containing CUI or other sensitive information in accordance with applicable organizational and/or federal standards and policies.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(5)	MEDIA SANITIZATION
MP-6(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization sanitizes information system media containing classified information in accordance with NSA standards and policies.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

MP-6(6)	MEDIA SANITIZATION
MP-6(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization implements the media destruction process for information system media that cannot be sanitized.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media sanitization responsibilities].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-1	**PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**
PE-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents physical and environmental protection policy;* *(ii) the organization physical and environmental protection policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities;* *(iv) the organization develops and formally documents physical and environmental protection procedures;* *(v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and* *(vi) the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical and environmental protection responsibilities].
PE-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of physical and environmental protection policy reviews/updates;* *(ii) the organization reviews/updates physical and environmental protection policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of physical and environmental protection procedure reviews/updates;* *(iv) the organization reviews/updates physical and environmental protection procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical and environmental protection responsibilities].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-2	**PHYSICAL ACCESS AUTHORIZATIONS**
PE-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies areas within the facility that are publicly accessible;* *(ii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and* *(iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; other relevant documents or records].
PE-2.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility;* *(ii) organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and* *(iii) the organization removes from the access list personnel no longer requiring access.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; other relevant documents or records].

PE-2(1)	**PHYSICAL ACCESS AUTHORIZATIONS**
PE-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies personnel positions or roles authorized for physical access to the facility where the information system resides; and* *(ii) the organization authorizes physical access to the facility where the information system resides based on position or role.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; physical access control logs or records; information system entry and exit points; other relevant documents or records].

PE-2(2)	PHYSICAL ACCESS AUTHORIZATIONS
PE-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires two forms of identification to gain access to the facility where the information system resides.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; physical access control logs or records; information system entry and exit points; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to information system facility].

PE-2(3)	PHYSICAL ACCESS AUTHORIZATIONS
PE-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies authorized personnel with appropriate clearances and access authorizations for gaining physical access to the facility containing an information system that processes classified information; and* *(ii) the organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; physical access control logs or records; information system entry and exit points; other relevant documents or records].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-3	**PHYSICAL ACCESS CONTROL**
PE-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);* *(ii) the organization verifies individual access authorizations before granting access to the facility;* *(iii) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;* *(iv) the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; and* *(v) the organization secures keys, combinations, and other physical access devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; storage locations for physical access devices; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical access control responsibilities]. **Test**: [*SELECT FROM:* Physical access control capability; physical access control devices].
PE-3.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for conducting inventories of physical access devices;* *(ii) the organization inventories physical access devices in accordance with the organization-defined frequency;* *(iii) the organization defines the frequency of changes to combinations and keys; and* *(iv) the organization changes combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records]. **Test**: [*SELECT FROM:* Physical access control devices].

PE-3(1)	PHYSICAL ACCESS CONTROL
PE-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records].

PE-3(2)	PHYSICAL ACCESS CONTROL
PE-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; records of security checks; facility layout documentation; information system entry and exit points; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical access control responsibilities].

PE-3(3)	PHYSICAL ACCESS CONTROL
PE-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; facility surveillance records; facility layout documentation; information system entry and exit points; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical access control responsibilities].

PE-3(4)	PHYSICAL ACCESS CONTROL
PE-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system components to be protected from unauthorized physical access using lockable physical casings; and* *(ii) the organization uses lockable physical casings to protect organization-defined information system components from unauthorized physical access.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; security plan; list of information system components requiring protection through lockable physical casings; lockable physical casings; other relevant documents or records].

PE-3(5)	PHYSICAL ACCESS CONTROL
PE-3(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system detects/prevents physical tampering or alteration of hardware components within the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system design documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Physical access control capability].

PE-3(6)	PHYSICAL ACCESS CONTROL
PE-3(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of unannounced attempts to be included in a penetration testing process to bypass or circumvent security controls associated with physical access points to the facility; and* *(ii) the organization employs a penetration testing process that includes unannounced attempts, in accordance with the organization-defined frequency, to bypass or circumvent security controls associated with physical access points to the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; procedures addressing penetration testing; rules of engagement and associated documentation; penetration test results; security plan; other relevant documents or records].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-4	**ACCESS CONTROL FOR TRANSMISSION MEDIUM**
PE-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; other relevant documents or records].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-5	**ACCESS CONTROL FOR OUTPUT DEVICES**
PE-5.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual displays from information system components; other relevant documents or records].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-6	**MONITORING PHYSICAL ACCESS**
PE-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization monitors physical access to the information system to detect and respond to physical security incidents;* *(ii) the organization defines the frequency to review physical access logs;* *(iii) the organization reviews physical access logs in accordance with the organization-defined frequency; and* *(iv) the organization coordinates results of reviews and investigations with the organization's incident response capability.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical access monitoring responsibilities]. **Test**: [*SELECT FROM:* Physical access monitoring capability].

PE-6(1)	MONITORING PHYSICAL ACCESS
PE-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization monitors real-time physical intrusion alarms and surveillance equipment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with physical access monitoring responsibilities]. **Test**: [*SELECT FROM:* Physical access monitoring capability].

PE-6(2)	MONITORING PHYSICAL ACCESS
PE-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access monitoring; information system design documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing physical access monitoring capability].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-7	**VISITOR CONTROL**
PE-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with visitor access control responsibilities]. **Test:** [*SELECT FROM:* Visitor access control capability].

PE-7(1)	**VISITOR CONTROL**
PE-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization escorts visitors and monitors visitor activity, when required.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with visitor access control responsibilities].

PE-7(2)	**VISITOR CONTROL**
PE-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires two forms of identification for visitor access to the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with visitor access control responsibilities].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-8	**ACCESS RECORDS**
PE-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);* *(ii) the organization defines the frequency to review visitor access records;* *(iii) the organization reviews the visitor access records in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for reviewing physical access records].

PE-8(1)	ACCESS RECORDS
PE-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to facilitate the maintenance and review of access records.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management of access records; facility access control logs or records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for reviewing physical access records].

PE-8(2)	ACCESS RECORDS
PE-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing facility access records; facility access control logs or records; other relevant documents or records].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-9	**POWER EQUIPMENT AND POWER CABLING**
PE-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records].

PE-9(1)	**POWER EQUIPMENT AND POWER CABLING**
PE-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs redundant and parallel power cabling paths.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records].

PE-9(2)	**POWER EQUIPMENT AND POWER CABLING**
PE-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the critical information system components that require automatic voltage controls; and* *(ii) the organization employs automatic voltage controls for organization-defined critical information system components* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing voltage control; security plan; list of critical information system components requiring automatic voltage controls; other relevant documents or records].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-10	**EMERGENCY SHUTOFF**
PE-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization provides the capability of shutting off power to the information system or individual system components in emergency situations;* *(ii) the organization defines the location of emergency shutoff switches or devices by information system or system component;* *(iii) the organization places emergency shutoff switches or devices in an organization-defined location by information system or system component to facilitate safe and easy access for personnel; and* *(iv) the organization protects the emergency power shutoff capability from unauthorized activation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; other relevant documents or records].

PE-10(1)	**EMERGENCY SHUTOFF** [Withdrawn: Incorporated into PE-10].
PE-10(1).1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into PE-10]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into PE-10].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-11	**EMERGENCY POWER**
PE-11.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; other relevant documents or records]. **Test:** [*SELECT FROM:* Uninterruptible power supply].

PE-11(1)	EMERGENCY POWER
PE-11(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records]. **Test:** [*SELECT FROM:* Alternate power supply].

PE-11(2)	EMERGENCY POWER
PE-11(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records]. **Test:** [*SELECT FROM:* Alternate power supply].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-12	**EMERGENCY LIGHTING**
PE-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;* *(ii) the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility; and* *(iii) the organization maintains the automatic emergency lighting for the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with emergency planning responsibilities]. **Test**: [*SELECT FROM:* Emergency lighting capability].

PE-12(1)	EMERGENCY LIGHTING
PE-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with emergency planning responsibilities]. **Test**: [*SELECT FROM:* Emergency lighting capability].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-13	**FIRE PROTECTION**
PE-13.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source; and* *(ii) the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems].

PE-13(1)	FIRE PROTECTION
PE-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs fire detection devices/systems for the information system that, without manual intervention, activate automatically and notify the organization and emergency responders in the event of a fire.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems]. **Test:** [*SELECT FROM:* Simulated activation of fire detection devices/systems and automated notifications].

PE-13(2)	FIRE PROTECTION
PE-13(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems]. **Test:** [*SELECT FROM:* Simulated activation of fire suppression devices/systems and automated notifications].

PE-13(3)	FIRE PROTECTION
PE-13(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems]. **Test**: [*SELECT FROM:* Simulated activation of fire suppression devices/systems].

PE-13(4)	FIRE PROTECTION
PE-13(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of fire marshal inspections for the facility;* *(ii) the facility undergoes fire marshal inspections in accordance with the organization-defined frequency; and* *(iii) the organization promptly resolves deficiencies identified by fire marshal inspections.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing fire protection; security plan; facility housing the information system; fire marshal inspection results; test records of fire suppression and detection devices/systems; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for fire detection and suppression devices/systems].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-14	**TEMPERATURE AND HUMIDITY CONTROLS**
PE-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;* *(ii) the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;* *(iii) the organization defines the frequency to monitor temperature and humidity levels; and* *(iv) the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records].

PE-14(1)	TEMPERATURE AND HUMIDITY CONTROLS
PE-14(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing temperature and humidity controls; facility housing the information system; automated mechanisms for temperature and humidity; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing temperature and humidity controls].

PE-14(2)	TEMPERATURE AND HUMIDITY CONTROLS
PE-14(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing temperature and humidity monitoring; facility housing the information system; logs or records of temperature and humidity monitoring; records of changes to temperature and humidity levels that generate alarms or notifications; other relevant documents or records]. **Test:** [*SELECT FROM:* Temperature and humidity monitoring capability].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-15	**WATER DAMAGE PROTECTION**
PE-15.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly; and* *(ii) key personnel within the organization have knowledge of the master water shutoff valves.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with physical and environmental protection responsibilities]. **Test:** [*SELECT FROM:* Master water-shutoff valves; process for activating master water-shutoff].

PE-15(1)	WATER DAMAGE PROTECTION
PE-15(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; automated mechanisms for water shutoff valves; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing master water shutoff valve activation].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-16	**DELIVERY AND REMOVAL**
PE-16.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of information system components to be authorized, monitored, and controlled as such components are entering or exiting the facility;* *(ii) the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility; and* *(iii) the organization maintains records of information system components entering and exiting the facility.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; security plan; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with responsibilities for controlling information system components entering and exiting the facility]. **Test:** [*SELECT FROM:* Process for controlling information system-related items entering and exiting the facility].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-17	**ALTERNATE WORK SITE**
PE-17.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the management, operational, and technical information system security controls to be employed at alternate work sites;* *(ii) the organization employs organization-defined management, operational, and technical information system security controls at alternate work sites;* *(iii) the organization assesses, as feasible, the effectiveness of security controls at alternate work sites; and* *(iv) the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organization personnel using alternate work sites].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-18	**LOCATION OF INFORMATION SYSTEM COMPONENTS**
PE-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and* *(ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records].

PE-18(1)	LOCATION OF INFORMATION SYSTEM COMPONENTS
PE-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards; and* *(ii) the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with site selection responsibilities for the facility housing the information system].

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PE-19	**INFORMATION LEAKAGE**
PE-19.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects the information system from information leakage due to electromagnetic signals emanations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signals emanations; mechanisms protecting the information system against electronic signals emanation; facility housing the information system; records from electromagnetic signals emanation tests; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system for information leakage due to electromagnetic signals emanations].

PE-19(1)	INFORMATION LEAKAGE
PE-19(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system components, associated data communications, and networks are protected in accordance with:* – *national emissions and TEMPEST policies and procedures; and* – *the sensitivity of the information being transmitted.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing information leakage that comply with national emissions and TEMPEST policies and procedures; information system component design documentation; information system configuration settings and associated documentation other relevant documents or records]. **Test:** [*SELECT FROM:* Information system components for compliance with national emissions and TEMPEST policies and procedures].

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-1	**SECURITY PLANNING POLICY AND PROCEDURES**
PL-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents security planning policy;* *(ii) the organization security planning policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;* *(iv) the organization develops and formally documents security planning procedures;* *(v) the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls; and* *(vi) the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security planning responsibilities].
PL-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of security planning policy reviews/updates;* *(ii) the organization reviews/updates security planning policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of security planning procedure reviews/updates;* *(iv) the organization reviews/updates security planning procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security planning policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security planning responsibilities].

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-2	**SYSTEM SECURITY PLAN**
PL-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a security plan for the information system that:* - *is consistent with the organization's enterprise architecture;* - *explicitly defines the authorization boundary for the system;* - *describes the operational context of the information system in terms of mission and business processes;* - *provides the security categorization of the information system including supporting rationale;* - *describes the operational environment for the information system;* - *describes relationships with or connections to other information systems;* - *provides an overview of the security requirements for the system;* - *describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions; and* - *is reviewed and approved by the authorizing official or designated representative prior to plan implementation;* *(ii) the organization defines the frequency of security plan reviews;* *(iii) the organization reviews the security plan in accordance with the organization-defined frequency; and* *(iv) the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with security planning and plan implementation responsibilities for the information system].

PL-2(1)	SYSTEM SECURITY PLAN
PL-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum:* - *the purpose of the system;* - *a description of the system architecture;* - *the security authorization schedule; and* - *the security categorization and associated factors considered in determining the categorization;* *(ii) the organization defines the frequency of reviews and updates to the CONOPS; and* *(iii) the organization reviews and updates the CONOPS in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing security CONOPS development; procedures addressing security CONOPS reviews and updates; security CONOPS for the information system; security plan for the information system; records of security CONOPS reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with security planning and plan implementation responsibilities for the information system].

PL-2(2)	SYSTEM SECURITY PLAN
PL-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops a functional architecture for the information system that identifies and maintains:* – *external interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;* – *user roles and the access privileges assigned to each role;* – *unique security requirements;* – *types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and* – *restoration priority of information or information system services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security planning policy; access control policy; contingency planning policy; security plan for the information system; contingency plan for the information system; information system design documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with security planning and plan implementation responsibilities for the information system].

FAMILY: PLANNING

CLASS: MANAGEMENT

ASSESSMENT PROCEDURE	
PL-3	**SYSTEM SECURITY PLAN UPDATE** [Withdrawn: Incorporated into PL-2].
PL-3.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into PL-2]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into PL-2].

FAMILY: PLANNING **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PL-4	**RULES OF BEHAVIOR**
PL-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;* *(ii) the organization makes the rules available to all information system users; and* *(iii) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel who are authorized users of the information system and have signed rules of behavior].

PL-4(1)	RULES OF BEHAVIOR
PL-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes in the rules of behavior:* – *explicit restrictions on the use of social networking sites;* – *posting information on commercial Web sites; and* – *sharing information system account information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel who are authorized users of the information system and have signed rules of behavior].

FAMILY: PLANNING

CLASS: MANAGEMENT

ASSESSMENT PROCEDURE	
PL-5	**PRIVACY IMPACT ASSESSMENT**
PL-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts a privacy impact assessment on the information system; and* *(ii) the privacy impact assessment is in accordance with OMB policy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records].

FAMILY: PLANNING

CLASS: MANAGEMENT

ASSESSMENT PROCEDURE	
PL-6	**SECURITY-RELATED ACTIVITY PLANNING**
PL-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with security planning and plan implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-1	**INFORMATION SECURITY PROGRAM PLAN**
PM-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops an information security program plan for the organization that:* - *provides an overview of the requirements for the security program;* - *provides a description of the security program management controls and common controls in place or planned for meeting security program requirements;* - *provides sufficient information about the program management controls and common controls (including specification of parameters for any* assignment *and* selection *operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;* - *includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;* - *is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation;* *(ii) the organization defines the frequency of information security program plan reviews;* *(iii) the organization reviews the organization-wide information security program plan in accordance with the organization-defined frequency;* *(iv) the organization revises the plan to address organizational changes and problems identified during plan implementation or security control assessments; and* *(v) the organization disseminates the most recent information security program plan to appropriate entities in the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security planning and plan implementation responsibilities for the information security program].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-2	**SENIOR INFORMATION SECURITY OFFICER**
PM-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) organization appoints a senior information security officer to coordinate, develop, implement, and maintain an organization-wide information security program; and* *(ii) the organization empowers the senior information security officer with the mission and resources required to coordinate, develop, implement, and maintain an organization-wide information security program.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational person appointed to the senior information security officer position].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-3	**INFORMATION SECURITY RESOURCES**
PM-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization includes in its capital planning and investment requests the resources needed to implement the information security program;* *(ii) the organization documents all exceptions to the requirement that all capital planning and investment requests include the resources needed to implement the information security program;* *(iii) the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and* *(iv) the organization makes the required information security resources available for expenditure as planned.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; Exhibit 300; Exhibit 53; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-4	**PLAN OF ACTION AND MILESTONES PROCESS**
PM-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization implements a process to maintain plans of action and milestones for the security program and the associated organizational information systems; and* *(ii) the organization implements a process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with plan of action and milestones development and implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-5	**INFORMATION SYSTEM INVENTORY**
PM-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops an inventory of its information systems; and* *(ii) the organization maintains an inventory of its information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information security program policy; procedures addressing information system inventory development and maintenance; information system inventory records, other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system inventory development and maintenance responsibilities].

FAMILY: PROGRAM MANAGEMENT

CLASS: MANAGEMENT

ASSESSMENT PROCEDURE	
PM-6	**INFORMATION SECURITY MEASURES OF PERFORMANCE**
PM-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops information security measures of performance;* *(ii) the organization monitors information security measures of performance; and* *(iii) the organization reports on the results of information security measures of performance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; procedures addressing development, monitoring, and reporting of information security performance measures; information security performance metrics; information security performance measures; results of information security performance measures; other relevant documents or records].

FAMILY: PROGRAM MANAGEMENT

CLASS: MANAGEMENT

ASSESSMENT PROCEDURE	
PM-7	**ENTERPRISE ARCHITECTURE**
PM-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records].

FAMILY: PROGRAM MANAGEMENT

CLASS: MANAGEMENT

ASSESSMENT PROCEDURE	
PM-8	**CRITICAL INFRASTRUCTURE PLAN**
PM-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and documents a critical infrastructure and key resource protection plan;* *(ii) the organization updates the critical infrastructure and key resource protection plan; and* *(iii) the organization addresses information security issues in the critical infrastructure and key resource protection plan.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information security program policy; critical infrastructure protection policy; procedures addressing critical infrastructure plan development and implementation; procedures addressing critical infrastructure plan reviews and updates; records of critical infrastructure plan reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with critical infrastructure plan development and implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-9	**RISK MANAGEMENT STRATEGY**
PM-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and* *(ii) the organization implements that strategy consistently across the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk management strategy development and implementation responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-10	**SECURITY AUTHORIZATION PROCESS**
PM-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;* *(ii) the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and* *(iii) the organization fully integrates the security authorization processes into an organization-wide risk management program.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities].

FAMILY: PROGRAM MANAGEMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
PM-11	**MISSION / BUSINESS PROCESS DEFINITION**
PM-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and* *(ii) the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Information security program policy; risk management policy; procedures addressing security categorization of organizational information and information systems; organizational mission/business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with mission/business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-1	**PERSONNEL SECURITY POLICY AND PROCEDURES**
PS-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents personnel security policy;* *(ii) the organization personnel security policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;* *(iv) the organization develops and formally documents personnel security procedures;* *(v) the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls; and* *(vi) the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy and procedures, other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].
PS-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of personnel security policy reviews/updates;* *(ii) the organization reviews/updates personnel security policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of personnel security procedure reviews/updates;* *(iv) the organization reviews/updates personnel security procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-2	**POSITION CATEGORIZATION**
PS-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization assigns a risk designation to all positions within the organization;* *(ii) the organization establishes a screening criteria for individuals filling organizational positions;* *(iii) the organization defines the frequency of risk designation reviews and updates for organizational positions; and* *(iv) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
PS-3	**PERSONNEL SCREENING**
PS-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization screens individuals prior to authorizing access to the information system;* *(ii) the organization defines conditions requiring re-screening and, where re-screening is so indicated, the frequency of such re-screening; and* *(iii) the organization re-screens individuals according to organization-defined conditions requiring re-screening and, where re-screening is so indicated, the organization-defined frequency of such re-screening.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

PS-3(1)	PERSONNEL SCREENING
PS-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization ensures that every user accessing an information system processing, storing, or transmitting classified information is cleared to the highest classification level of the information on the system; and* *(ii) the organization ensures that every user accessing an information system processing, storing, or transmitting classified information is indoctrinated to the highest classification level of the information on the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

PS-3(2)	PERSONNEL SCREENING
PS-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization formally indoctrinates every user accessing an information system that processes, stores, or transmits types of classified information requiring formal indoctrination for all of the relevant types of information on the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
PS-4	**PERSONNEL TERMINATION**
PS-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization terminates information system access upon termination of individual employment;* *(ii) the organization conducts exit interviews of terminated personnel;* *(iii) the organization retrieves all security-related organizational information system-related property from terminated personnel; and* *(iv) the organization retains access to organizational information and information systems formerly controlled by terminated personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
PS-5	**PERSONNEL TRANSFER**
PS-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;* *(ii) the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment; and* *(iii) the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
PS-6	**ACCESS AGREEMENTS**
PS-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies appropriate access agreements for individuals requiring access to organizational information and information systems;* *(ii) individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;* *(iii) the organization defines the frequency of reviews/updates for access agreements; and* *(iv) the organization reviews/updates the access agreements in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Personnel security policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

PS-6(1)	**ACCESS AGREEMENTS**
PS-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization grants access to information with special protection measures only to individuals who:* – *have a valid access authorization that is demonstrated by assigned official government duties; and* – *satisfy associated personnel security criteria.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Personnel security policy; procedures addressing access agreements for organizational information and information systems; access agreements; access authorizations; personnel security criteria; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

PS-6(2)	ACCESS AGREEMENTS
PS-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization grants access to classified information with special protection measures only to individuals who:* – *have a valid access authorization that is demonstrated by assigned official government duties;* – *satisfy associated personnel security criteria; and* – *have read, understood, and signed a nondisclosure agreement.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing access agreements for organizational information and information systems; access agreements; access authorizations; personnel security criteria; signed nondisclosure agreements; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
PS-7	**THIRD-PARTY PERSONNEL SECURITY**
PS-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;* *(ii) the organization documents personnel security requirements for third-party providers; and* *(iii) the organization monitors third-party provider compliance with personnel security requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities; third-party providers].

FAMILY: PERSONNEL SECURITY

CLASS: OPERATIONAL

ASSESSMENT PROCEDURE	
PS-8	**PERSONNEL SANCTIONS**
PS-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with personnel security responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-1	**RISK ASSESSMENT POLICY AND PROCEDURES**
RA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents risk assessment policy;* *(ii) the organization risk assessment policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;* *(iv) the organization develops and formally documents risk assessment procedures;* *(v) the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; and* *(vi) the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities].
RA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of risk assessment policy reviews/updates;* *(ii) the organization reviews/updates risk assessment policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of risk assessment procedure reviews/updates;* *(iv) the organization reviews/updates risk assessment procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-2	**SECURITY CATEGORIZATION**
RA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;* *(ii) the organization documents the security categorization results (including supporting rationale) in the security plan for the information system; and* *(iii) the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security categorization and risk assessment responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-3	**RISK ASSESSMENT**
RA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:* - *access;* - *use;* - *disclosure;* - *disruption;* - *modification; or* - *destruction;* *(ii) the organization defines the document in which risk assessment results are documented, selecting from the security plan, risk assessment report, or other organization-defined document;* *(iii) the organization documents risk assessment results in the organization-defined document;* *(iv) the organization defines the frequency for review of the risk assessment results;* *(v) the organization reviews risk assessment results in accordance with the organization-defined frequency;* *(vi) the organization defines the frequency that risk assessments are updated; and* *(vii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-4	**RISK ASSESSMENT UPDATE** [Withdrawn: Incorporated into RA-3].
RA-4.1	**ASSESSMENT OBJECTIVE:** [Withdrawn: Incorporated into RA-3]. **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** [Withdrawn: Incorporated into RA-3].

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
RA-5	**VULNERABILITY SCANNING**
RA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines:* - *the frequency for conducting vulnerability scans on the information system and hosted applications and/or;* - *the organization-defined process for conducting random vulnerability scans on the information system and hosted applications;* *(ii) the organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency and/or the organization-defined process for random scans;* *(iii) the organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported;* *(iv) the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:* - *enumerating platforms, software flaws, and improper configurations;* - *formatting/and making transparent checklists and test procedures; and* - *measuring vulnerability impact, and* *(v) the organization analyzes vulnerability scan reports and results from security control assessments.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].
RA-5.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the response times for remediating legitimate vulnerabilities in accordance with an organizational assessment of risk;* *(ii) the organization remediates legitimate vulnerabilities in accordance with organization-defined response times; and* *(iii) the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment and vulnerability scanning responsibilities].

RA-5(1)	VULNERABILITY SCANNING
RA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; other relevant documents or records]. **Test**: [*SELECT FROM:* Vulnerability scanning capability and associated scanning tools].

RA-5(2)	VULNERABILITY SCANNING
RA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of updates for information system vulnerabilities scanned; and* *(ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when new vulnerabilities are identified and reported.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records].

RA-5(3)	VULNERABILITY SCANNING
RA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs vulnerability scanning procedures that can demonstrate the breadth of coverage (i.e., information system components scanned); and* *(ii) the organization employs vulnerability scanning procedures that can demonstrate the depth of coverage (i.e., vulnerabilities checked).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records].

RA-5(4)	VULNERABILITY SCANNING
RA-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization attempts to discern what information about the information system is discoverable by adversaries.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; penetration test results; vulnerability scanning results; other relevant documents or records].

RA-5(5)	VULNERABILITY SCANNING
RA-5(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the list of information system components to which privileged access is authorized for selected vulnerability scanning activities; and* *(ii) the organization includes privileged access authorization to organization-defined information system components identified for selected vulnerability scanning activities to facilitate more thorough scanning.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; security plan; list of information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; other relevant documents or records].

RA-5(6)	VULNERABILITY SCANNING
RA-5(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; vulnerability scanning results; other relevant documents or records]. **Test**: [*SELECT FROM:* Vulnerability scanning capability and associated scanning tools].

RA-5(7)	VULNERABILITY SCANNING
RA-5(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for employing automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials; and* *(ii) the organization employs automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated officials in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; security plan; information system design documentation; list of unauthorized software; notifications or alerts of unauthorized software on organizational information systems; other relevant documents or records]. **Test**: [*SELECT FROM:* Vulnerability scanning capability and associated scanning tools].

RA-5(8)	VULNERABILITY SCANNING
RA-5(8).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; audit logs; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with vulnerability scanning responsibilities].

RA-5(9)	VULNERABILITY SCANNING
RA-5(9).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an independent penetration agent or penetration team to:* – *conduct a vulnerability analysis on the information system; and* – *perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* Risk assessment policy; security assessment policy; procedures addressing vulnerability analysis; risk assessment; security plan; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with vulnerability scanning and analysis responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-1	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**
SA-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system services and acquisition policy;* *(ii) the organization system services and acquisition policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities;* *(iv) the organization develops and formally documents system services and acquisition procedures;* *(v) the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls; and* *(vi) the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities].
SA-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system services and acquisition policy reviews/updates;* *(ii) the organization reviews/updates system services and acquisition policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of system services and acquisition procedure reviews/updates;* *(iv) the organization reviews/updates system services and acquisition procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-2	**ALLOCATION OF RESOURCES**
SA-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization includes a determination of the information security requirements for the information system in mission/business process planning;* *(ii) the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and* *(iii) the organization establishes a discrete line item for information security in organizational programming and budgeting documentation.* **ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; organizational programming and budgeting documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with capital planning and investment responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-3	**LIFE CYCLE SUPPORT**
SA-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization manages the information system using a system development life cycle methodology that includes information security considerations;* *(ii) the organization defines and documents information system security roles and responsibilities throughout the system development life cycle; and* *(iii) the organization identifies individuals having information system security roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information security and system life cycle development responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-4	**ACQUISITIONS**
SA-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:* – *security functional requirements/specifications;* – *security-related documentation requirements; and* – *developmental and evaluation-related assurance requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities].

SA-4(1)	ACQUISITIONS
SA-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires in acquisition documents that vendors/contractors provide information describing in the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-4(2)	ACQUISITIONS
SA-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-4(3)	ACQUISITIONS
SA-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires software vendors/manufacturers to minimize flawed or malformed software by demonstrating that their software development processes employ:* – *state-of-the-practice software and security engineering methods;* – *quality control processes; and* – *validation techniques.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-4(4)	ACQUISITIONS
SA-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization explicitly assigns each acquired information system component to an information system; and* *(ii) the owner of the system acknowledges each assignment of information system components to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; information system owner].

SA-4(5)	ACQUISITIONS
SA-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires in acquisition documents that information system components are delivered in a secure, documented configuration; and* *(ii) the organization requires in acquisition documents that the secure configuration is the default configuration for any software reinstalls or upgrades.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-4(6)	ACQUISITIONS
SA-4(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and* *(ii) the organization ensures that these products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities].

SA-4(7)	ACQUISITIONS
SA-4(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization limits the use of commercially-provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists;* *(ii) the organization requires a commercially-provided information technology product to rely on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type; and* *(iii) the organization requires the use of a FIPS-validated, cryptographic module for a technology product that relies on cryptographic functionality to enforce its security policy when no U.S. Government Protection Profile exists for such a specific technology type.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-5	**INFORMATION SYSTEM DOCUMENTATION**
SA-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:* - *secure configuration, installation, and operation of the information system;* - *effective use and maintenance of the security features/functions; and* - *known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;* *(ii) the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:* - *user-accessible security features/functions and how to effectively use those security features/functions;* - *methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and* - *user responsibilities in maintaining the security of the information and information system; and* *(iii) the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(1)	INFORMATION SYSTEM DOCUMENTATION
SA-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(2)	INFORMATION SYSTEM DOCUMENTATION
SA-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(3)	INFORMATION SYSTEM DOCUMENTATION
SA-5(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(4)	INFORMATION SYSTEM DOCUMENTATION
SA-5(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-5(5)	INFORMATION SYSTEM DOCUMENTATION
SA-5(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization obtains, protects as required, and makes available to authorized personnel, the source code for the information system to permit analysis and testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing information system documentation; information system design documentation; information system source code documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and/or maintaining the information system].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-6	**SOFTWARE USAGE RESTRICTIONS**
SA-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization uses software and associated documentation in accordance with contract agreements and copyright laws;* *(ii) the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and* *(iii) the organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system].

SA-6(1)	SOFTWARE USAGE RESTRICTIONS
SA-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code;* *(ii) the organization provides exceptions to the source code requirement only when no alternative solutions are available to support compelling mission/operational requirements; and* *(iii) the organization obtains express written consent of the authorizing official for exceptions to the source code requirement.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-7	**USER-INSTALLED SOFTWARE**
SA-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users; and* *(ii) the organization (or information system) enforces explicit rules governing the installation of software by users.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system]. **Test**: [*SELECT FROM:* Enforcement of rules for user installed software on the information system; information system for prohibited software].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-8	**SECURITY ENGINEERING PRINCIPLES**
SA-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) The organization applies information system security engineering principles in the specification of the information system;* *(ii) the organization applies information system security engineering principles in the design of the information system;* *(iii) the organization applies information system security engineering principles in the development of the information system;* *(iv) the organization applies information system security engineering principles in the implementation of the information system; and* *(v) the organization applies information system security engineering principles in the modification of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system design, development, implementation, and modification responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-9	**EXTERNAL INFORMATION SYSTEM SERVICES**
SA-9.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;* *(ii) the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services; and* *(iii) the organization monitors security control compliance by external service providers.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities; external providers of information system services].

SA-9(1)	**SOFTWARE USAGE RESTRICTIONS**
SA-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services;* *(ii) the organization defines the senior organizational official designated to approve the acquisition or outsourcing of dedicated information security services; and* *(iii) the designated senior organizational official approves the acquisition or outsourcing of dedicated information security services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; risk assessment reports; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-10	**DEVELOPER CONFIGURATION MANAGEMENT**
SA-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators:* *(i) perform configuration management during information system:* - *design;* - *development;* - *implementation; and* - *operation;* *(ii) manage and control changes to the information system during:* - *design;* - *development;* - *implementation; and* - *modification;* *(iii) implement only organization-approved changes;* *(iv) document approved changes to the information system; and* *(v) track security flaws and flaw resolution.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].

SA-10(1)	**DEVELOPER CONFIGURATION MANAGEMENT**
SA-10(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records].

SA-10(2)	DEVELOPER CONFIGURATION MANAGEMENT
SA-10(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization provides an alternative configuration management process with organizational personnel in the absence of a dedicated developer/integrator configuration management team.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

	ASSESSMENT PROCEDURE
SA-11	**DEVELOPER SECURITY TESTING**
SA-11.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):* – *create and implement a security test and evaluation plan;* – *implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and* – *document the results of the security testing/evaluation and flaw remediation processes.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with developer security testing responsibilities].

SA-11(1)	**DEVELOPER SECURITY TESTING**
SA-11(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws; and* *(ii) the organization requires that information system developers/integrators document the results of the analysis.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with developer security testing responsibilities].

SA-11(2)	DEVELOPER SECURITY TESTING
SA-11(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; vulnerability scanning results; information system risk assessment report; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with developer security testing responsibilities].

SA-11(3)	DEVELOPER SECURITY TESTING
SA-11(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization requires that information system developers/integrators create a security test and evaluation plan; and* *(ii) the organization requires that information system developers/integrators implement the plan under the witness of an independent verification and validation agent.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing information system developer/integrator security testing; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; security test and evaluation plan; security test and evaluation results report; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system security, acquisition, and contracting responsibilities; organizational personnel with developer security testing responsibilities; independent verification and validation agent].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

	ASSESSMENT PROCEDURE
SA-12	**SUPPLY CHAIN PROTECTION**
SA-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the measures to be employed to protect against supply chain threats; and* *(ii) the organization protects against supply chain threats by employing organization-defined measures as part of a comprehensive, defense-in-breadth information security strategy.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; information system development life cycle documentation; other relevant documents or records].

SA-12(1)	**SUPPLY CHAIN PROTECTION**
SA-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization purchases all anticipated information system components and spares in the initial acquisition.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-12(2)	**SUPPLY CHAIN PROTECTION**
SA-12(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; due diligence reviews documentation; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with supply chain protection responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities].

SA-12(3)	SUPPLY CHAIN PROTECTION
SA-12(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization uses trusted shipping and warehousing for:* – *information systems;* – *information system components; and* – *information technology products.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with supply chain protection responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities].

SA-12(4)	SUPPLY CHAIN PROTECTION
SA-12(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs a diverse set of suppliers for:* – *information systems;* – *information system components;* – *information technology products; and* – *information system services.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-12(5)	SUPPLY CHAIN PROTECTION
SA-12(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs standard configurations for:* – *information systems;* – *information system components; and* – *information technology products.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; configuration management policy; procedures addressing the baseline configuration of the information system; configuration management plan; information system design documentation; information system architecture and configuration documentation; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records].

SA-12(6)	SUPPLY CHAIN PROTECTION
SA-12(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization minimizes the time between purchase decisions and delivery of:* – *information systems;* – *information system components; and* – *information technology products.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; shipment records; other relevant documents or records].

SA-12(7)	SUPPLY CHAIN PROTECTION
SA-12(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs independent analysis and penetration testing against delivered:* – *information systems;* – *information system components; and* – *information technology products.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; penetration testing records; security test and evaluation results reports; other relevant documents or records].

FTC-0002655

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-13	**TRUSTWORTHINESS**
SA-13.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the organization's level of trustworthiness; and* *(ii) the organization requires that the information system meet the organization-defined level of trustworthiness.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; penetration test and vulnerability scan reports; security test and evaluation results; authority to operate documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with system and services acquisition responsibilities; information system authorizing official].

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

ASSESSMENT PROCEDURE	
SA-14	**CRITICAL INFORMATION SYSTEM COMPONENTS**
SA-14.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the critical information system components that require re-implementation; and* *(ii) the organization re-implements organization-defined critical information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; configuration management plan; list of critical information system components requiring re-implementation; configuration baseline for critical information system components; configuration management records; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel implementing, operating, and/or maintaining the information system].

SA-14(1)	CRITICAL INFORMATION SYSTEM COMPONENTS
SA-14(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies information system components for which alternative sourcing is not viable;* *(ii) the organization defines the measures to be employed to prevent critical security controls for information system components from being compromised; and* *(iii) the organization employs organization-defined measures to ensure that critical security controls for information system components are not compromised.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and services acquisition policy; information system design documentation; information system configuration settings and associated documentation; list of information system components; security requirements and security specifications for the information system; penetration test and vulnerability scan reports; security test and evaluation results; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-1	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**
SC-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system and communications protection policy;* *(ii) the organization system and communications protection policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities;* *(iv) the organization develops and formally documents system and communications protection procedures;* *(v) the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls; and* *(vi) the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and communications protection responsibilities].
SC-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system and communications protection policy reviews/updates;* *(ii) the organization reviews/updates system and communications protection policy in accordance with organization-defined frequency; and* *(iii) the organization defines the frequency of system and communications protection procedure reviews/updates;* *(iv) the organization reviews/updates system and communications protection procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and communications protection responsibilities].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-2	**APPLICATION PARTITIONING**
SC-2.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system separates user functionality (including user interface services) from information system management functionality.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Separation of user functionality from information system management functionality].

SC-2(1)	**APPLICATION PARTITIONING**
SC-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Separation of user functionality from information system management functionality].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-3	**SECURITY FUNCTION ISOLATION**
SC-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions of the information system to be isolated from nonsecurity functions; and* *(ii) the information system isolates security functions from nonsecurity functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from nonsecurity functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Separation of security functions from nonsecurity functions within the information system].

SC-3(1)	SECURITY FUNCTION ISOLATION
SC-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements underlying hardware separation mechanisms to facilitate security function isolation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Hardware separation mechanisms facilitating security function isolation].

SC-3(2)	SECURITY FUNCTION ISOLATION
SC-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system isolates security functions enforcing access and information flow control from both nonsecurity functions and other security functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Isolation of security functions enforcing access and information flow control].

SC-3(3)	SECURITY FUNCTION ISOLATION
SC-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

SC-3(4)	SECURITY FUNCTION ISOLATION
SC-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

SC-3(5)	SECURITY FUNCTION ISOLATION
SC-3(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-4	**INFORMATION IN SHARED RESOURCES**
SC-4.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system for unauthorized and unintended transfer of information via shared system resources].

SC-4(1)	**INFORMATION IN SHARED RESOURCES**
SC-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system does not share resources that are used to interface with systems operating at different security levels.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-5	**DENIAL OF SERVICE PROTECTION**
SC-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and* *(ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system for protection against or limitation of the effects of denial of service attacks].

SC-5(1)	DENIAL OF SERVICE PROTECTION
SC-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system for protection against or limitation of the effects of denial of service attacks].

SC-5(2)	DENIAL OF SERVICE PROTECTION
SC-5(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing information system bandwidth, capacity, and redundancy management].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-6	**RESOURCE PRIORITY**
SC-6.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system limits the use of resources by priority.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing resource allocation capability].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-7	**BOUNDARY PROTECTION**
SC-7.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the external boundary of the information system;* *(ii) the organization defines key internal boundaries of the information system;* *(iii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system; and* *(iv) the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Selected organizational personnel with boundary protection responsibilities]. **Test:** [*SELECT FROM:* Automated mechanisms implementing boundary protection capability within the information system].

SC-7(1)	**BOUNDARY PROTECTION**
SC-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].

SC-7(2)	BOUNDARY PROTECTION
SC-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the mediation necessary for public access to the organization's internal networks; and* *(ii) the information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access controls for public access to the organization's internal networks].

SC-7(3)	BOUNDARY PROTECTION
SC-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; communications and network traffic monitoring logs; other relevant documents or records].

SC-7(4)	BOUNDARY PROTECTION
SC-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency for reviewing exceptions to traffic flow policy;* *(ii) the organization implements a managed interface for each external telecommunication service;* *(iii) the organization establishes a traffic flow policy for each managed interface;* *(iv) the organization employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;* *(v) the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;* *(vi) the organization reviews exceptions to the traffic flow policy in accordance with the organization-defined frequency; and* *(vii) the organization removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; traffic flow policy; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow policy exceptions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Selected organizational personnel with boundary protection responsibilities]. **Test**: [*SELECT FROM:* Managed interfaces implementing organizational traffic flow policy].

SC-7(5)	BOUNDARY PROTECTION
SC-7(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system, at managed interfaces, denies network traffic by default; and* *(ii) the information system, at managed interfaces, allows network traffic by exception.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Selected organizational personnel with boundary protection responsibilities].

SC-7(6)	BOUNDARY PROTECTION
SC-7(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization prevents the unauthorized release of information outside of the information system boundary; or* *(ii) the organization prevents any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms supporting the fail-safe boundary protection capability within the information system].

SC-7(7)	BOUNDARY PROTECTION
SC-7(7).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms supporting non-remote connections with the information system].

SC-7(8)	BOUNDARY PROTECTION
SC-7(8).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the internal communications traffic to be routed to external networks;* *(ii) the organization defines the external networks to which the organization-defined internal communications traffic should be routed; and* *(iii) the information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Mechanisms implementing managed interfaces within information system boundary protection devices].

SC-7(9)	BOUNDARY PROTECTION
SC-7(9).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system, at managed interfaces, denies network traffic; and* *(ii) the information system audits internal users (or malicious code) posing a threat to external information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Mechanisms implementing managed interfaces within information system boundary protection devices].

SC-7(10)	BOUNDARY PROTECTION
SC-7(10).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization prevents the unauthorized exfiltration of information across managed interfaces.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms preventing unauthorized exfiltration of information across managed interfaces].

SC-7(11)	BOUNDARY PROTECTION
SC-7(11).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system checks incoming communications to ensure:* *– the communications are coming from an authorized source; and* *– the communications are routed to an authorized destination.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].

SC-7(12)	BOUNDARY PROTECTION
SC-7(12).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements host-based boundary protection mechanisms for:* – *servers;* – *workstations; and* – *mobile devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing host-based boundary protection capability].

SC-7(13)	BOUNDARY PROTECTION
SC-7(13).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the key information security tools, mechanisms, and support components to be isolated from other internal information system components; and* *(ii) the organization isolates organization-defined key information security tools, mechanisms, and support components from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal information system components; other relevant documents or records].

SC-7(14)	BOUNDARY PROTECTION
SC-7(14).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the managed interfaces where boundary protections are to be implemented;* *(ii) the organization defines the measures to protect against unauthorized physical connections across boundary protections implemented at organization-defined managed interfaces; and* *(iii) the organization protects against unauthorized physical connections across the boundary protections implemented at organization-defined managed interfaces.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; facility communications and wiring diagram; other relevant documents or records]. **Test:** [*SELECT FROM:* Physical access capability implementing protections against unauthorized physical connections to the information system].

SC-7(15)	BOUNDARY PROTECTION
SC-7(15).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system routes all networked, privileged accesses through a dedicated, managed interface for purpose of access control; and* *(ii) the information system routes all networked, privileged accesses through a dedicated, managed interface for purpose of auditing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; audit logs; other relevant documents or records]. **Test:** [*SELECT FROM:* Mechanisms routing networked, privileged access through dedicated managed interfaces].

SC-7(16)	BOUNDARY PROTECTION
SC-7(16).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents discovery of specific system components (or devices) composing a managed interface.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Mechanisms preventing discovery of system components at a managed interface].

SC-7(17)	BOUNDARY PROTECTION
SC-7(17).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to enforce strict adherence to protocol format.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].

SC-7(18)	BOUNDARY PROTECTION
SC-7(18).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system fails securely in the event of an operational failure of a boundary protection device.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-8	**TRANSMISSION INTEGRITY**
SC-8.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the integrity of transmitted information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Transmission integrity capability within the information system].

SC-8(1)	**TRANSMISSION INTEGRITY**
SC-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Cryptographic mechanisms implementing transmission integrity capability within the information system].

SC-8(2)	**TRANSMISSION INTEGRITY**
SC-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system in preparation for transmission maintains the integrity of information during:* – *aggregation;* – *packaging; and* – *transformation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Transmission integrity capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-9	**TRANSMISSION CONFIDENTIALITY**
SC-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the confidentiality of transmitted information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Transmission confidentiality capability within the information system].

SC-9(1)	**TRANSMISSION CONFIDENTIALITY**
SC-9(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization optionally defines alternative physical measures to prevent unauthorized disclosure of information during transmission ; and* *(ii) the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organization-defined alternative physical measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Cryptographic mechanisms implementing transmission confidentiality capability within the information system].

SC-9(2)	**TRANSMISSION CONFIDENTIALITY**
SC-9(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system in preparation for transmission maintains the confidentiality of information during:* – *aggregation;* – *packaging; and* – *transformation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Transmission confidentiality capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-10	**NETWORK DISCONNECT**
SC-10.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period of inactivity before the information system terminates a network connection associated with a communications session; and* *(ii) the information system terminates a network connection associated with a communication session at the end of the session or after the organization-defined time period of inactivity.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Network disconnect capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-11	**TRUSTED PATH**
SC-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the security functions within the information system to be included in a trusted communications path;* *(ii) the organization-defined security functions include information system authentication and reauthentication; and* *(iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing trusted communications paths; security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing trusted communications paths within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-12	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
SC-12.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for cryptographic key establishment or management]. **Test:** [*SELECT FROM:* Automated mechanisms implementing cryptographic key management and establishment within the information system].

SC-12(1)	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
SC-12(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization maintains availability of information in the event of the loss of cryptographic keys by users.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

SC-12(2)	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**
SC-12(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines whether it will use NIST-approved or NSA-approved key management technology and processes; and* *(ii) the organization produces, controls, and distributes symmetric cryptographic keys using the organization-defined key management technology and processes.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for cryptographic key establishment or management].

SC-12(3)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
SC-12(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for cryptographic key establishment or management].

SC-12(4)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
SC-12(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; information system cryptographic keys; other relevant documents or records].

SC-12(5)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
SC-12(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; information system cryptographic keys; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-13	**USE OF CRYPTOGRAPHY**
SC-13.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records].

SC-13(1)	**USE OF CRYPTOGRAPHY**
SC-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records].

SC-13(2)	**USE OF CRYPTOGRAPHY**
SC-13(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs NSA-approved cryptography to protect classified information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of cryptography; NSA cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records].

SC-13(3)	USE OF CRYPTOGRAPHY
SC-13(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; FIPS cryptographic module validation certificates; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for implementing cryptography within the information system].

SC-13(4)	USE OF CRYPTOGRAPHY
SC-13(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines whether it will use NIST-approved or NSA-approved cryptography to implement digital signatures; and* *(ii) the organization employs the organization-defined cryptography to implement digital signatures* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-14	**PUBLIC ACCESS PROTECTIONS**
SC-14.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the integrity and availability of publicly available information and applications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms protecting the integrity and availability of publicly available information and applications within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-15	**COLLABORATIVE COMPUTING DEVICES**
SC-15.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines exceptions to the prohibiting of collaborative computing devices where remote activation is to be allowed;* *(ii) the organization prohibits remote activation of collaborative computing devices, excluding the organization-defined exceptions where remote activation is to be allowed; and* *(iii) the organization provides an explicit indication of use to users physically present at the devices.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users].

SC-15(1)	COLLABORATIVE COMPUTING DEVICES
SC-15(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Physical disconnect of collaborative computing devices].

SC-15(2)	COLLABORATIVE COMPUTING DEVICES
SC-15(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Mechanisms blocking inbound and outbound traffic between instant message clients that are independently configured].

SC-15(3)	COLLABORATIVE COMPUTING DEVICES
SC-15(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the secure work areas where collaborative computing devices are prohibited; and* *(ii) the organization disables or removes collaborative computing devices from information systems in organization-defined secure work areas.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM*: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM*: Organizational personnel with device management responsibilities for collaborative computing].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-16	**TRANSMISSION OF SECURITY ATTRIBUTES**
SC-16.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system associates security attributes with information exchanged between information systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms supporting reliable transmission of security parameters between information systems].

SC-16(1)	**TRANSMISSION OF SECURITY ATTRIBUTES**
SC-16(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system validates the integrity of security attributes exchanged between systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms supporting reliable transmission of security parameters between information systems].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-17	**PUBLIC KEY INFRASTRUCTURE CERTIFICATES**
SC-17.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines a certificate policy for issuing public key certificates; and* *(ii) the organization issues public key certificates under the organization-defined certificate policy or obtains public key certificates under a certificate policy from an approved service provider.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with public key infrastructure certificate issuing responsibilities].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-18	**MOBILE CODE**
SC-18.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines acceptable and unacceptable mobile code and mobile code technologies;* *(ii) the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and* *(iii) the organization authorizes, monitors, and controls the use of mobile code within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with mobile code authorization, monitoring, and control responsibilities]. **Test**: [*SELECT FROM:* Mobile code authorization and monitoring capability for the organization].

SC-18(1)	MOBILE CODE
SC-18(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system implements detection and inspection mechanisms to identify unauthorized mobile code; and* *(ii) the information system takes corrective action when unauthorized mobile code is identified.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing mobile code detection and inspection capability].

SC-18(2)	MOBILE CODE
SC-18(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines requirements for the acquisition, development and/or use of mobile code; and* *(ii) the organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets the organization-defined mobile code requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with mobile code management responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities].

SC-18(3)	MOBILE CODE
SC-18(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents the download and execution of prohibited mobile code.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms preventing download and execution of prohibited mobile code].

SC-18(4)	MOBILE CODE
SC-18(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines software applications for which automatic mobile code execution is to be prohibited;* *(ii) the organization defines actions required by the information system before executing mobile code;* *(iii) the information system prevents the automatic execution of mobile code in the organization-defined software applications; and* *(iv) the information system requires organization-defined actions before executing mobile code.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; information system design documentation; information system configuration settings and associated documentation; list of applications for which automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms preventing mobile code execution within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-19	**VOICE OVER INTERNET PROTOCOL**
SC-19.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and* *(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with VoIP authorization and monitoring responsibilities]. **Test**: [*SELECT FROM:* VoIP authorization and monitoring capability for the organization].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-20	**SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**
SC-20.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing secure name/address resolution service (authoritative source)].

SC-20(1)	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
SC-20(1).1	**ASSESSMENT OBJECTIVE:** *Determine if* *(i) the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces; and* *(ii) the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-21	**SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**
SC-21.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing data origin authentication and integrity verification for resolution services].

SC-21(1)	**SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**
SC-21(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system performs data origin authentication and data integrity verification on all resolution responses received whether or not client systems explicitly request this service.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing data origin authentication and integrity verification for resolution services].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-22	**ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**
SC-22.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information systems that collectively provide name/address resolution service for an organization are fault tolerant; and* *(ii) the information systems that collectively provide name/address resolution service for an organization implement internal/external role separation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms supporting name/address resolution service for fault tolerance and role separation].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-23	**SESSION AUTHENTICITY**
SC-23.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides mechanisms to protect the authenticity of communications sessions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing session authenticity].

SC-23(1)	SESSION AUTHENTICITY
SC-23(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system invalidates session identifiers upon user logout or other session termination.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing session identifier invalidation upon session termination].

SC-23(2)	SESSION AUTHENTICITY
SC-23(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides a readily observable logout capability whenever authentication is used to gain access to Web pages.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; information system site designs; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing logout capability for Web pages requiring user authentication].

SC-23(3)	SESSION AUTHENTICITY
SC-23(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system generates a unique session identifier for each session; and* *(ii) the information system recognizes only session identifiers that are system-generated.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms generating and monitoring unique session identifiers].

SC-23(4)	SESSION AUTHENTICITY
SC-23(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines requirements for randomly generating unique session identifiers; and* *(ii) the information system generates unique session identifiers in accordance with organization-defined randomness requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms generating unique session identifiers].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-24	**FAIL IN KNOWN STATE**
SC-24.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the known-states the information system should fail to in the event of a system failure;* *(ii) the organization defines types of failures for which the information system should fail to an organization-defined known-state;* *(iii) the organization defines the system state information that should be preserved in the event of a system failure;* *(iv) the information system fails to an organization-defined known-state for an organization-defined type of failure; and* *(v) the information system preserves organization-defined system state information in the event of a system failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing information system failure; information system design documentation; information system configuration settings and associated documentation; list of failures requiring information system to fail in a known state; state information to be preserved in system failure; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing fail-in-known-state capability].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-25	**THIN NODES**
SC-25.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system employs processing components that have minimal functionality and information storage.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of thin nodes; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-26	**HONEYPOTS**
SC-26.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of honeypots; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].

SC-26(1)	**HONEYPOTS**
SC-26(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system includes components that proactively seek to identify Web-based malicious code.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing use of honeypots; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms proactively seeking Web-based malicious code].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-27	**OPERATING SYSTEM-INDEPENDENT APPLICATIONS**
SC-27.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines applications that are operating system-independent; and* *(ii) the information system includes organization-defined operating system-independent applications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing operating system-independent applications; information system design documentation; information system configuration settings and associated documentation; list of operating system-independent applications; other relevant documents or records].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-28	**PROTECTION OF INFORMATION AT REST**
SC-28.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system protects the confidentiality and integrity of information at rest.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records]. **Test:** [*SELECT FROM:* Automated mechanisms implementing confidentiality and integrity protections for information at-rest].

SC-28(1)	**PROTECTION OF INFORMATION AT REST**
SC-28(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures; and* *(ii) the organization employs cryptographic mechanisms to prevent unauthorized modification of information at rest unless otherwise protected by alternative physical measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Cryptographic mechanisms implementing confidentiality and integrity protections for information at-rest].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-29	**HETEROGENEITY**
SC-29.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs diverse information technologies in the implementation of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; list of technologies deployed in the information system; acquisition documentation; acquisition contracts for information system components or services; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system acquisition, development, and implementation responsibilities].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-30	**VIRTUALIZATION TECHNIQUES**
SC-30.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of virtualization techniques to be employed for organizational information systems; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for implementing approved virtualization techniques for information systems].

SC-30(1)	**VIRTUALIZATION TECHNIQUES**
SC-30(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of changes to operating systems and applications through the use of virtualization techniques; and* *(ii) the organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; configuration management policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system architecture; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for implementing approved virtualization techniques for information systems].

SC-30(2)	**VIRTUALIZATION TECHNIQUES**
SC-30(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs randomness in the implementation of the virtualization techniques.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with responsibilities for implementing approved virtualization techniques for information systems].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-31	**COVERT CHANNEL ANALYSIS**
SC-31.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing covert channel analysis; information system design documentation; information system configuration settings and associated documentation; covert channel analysis documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with covert channel analysis responsibilities; information system developers/integrators].

SC-31(1)	**COVERT CHANNEL ANALYSIS**
SC-31(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization tests a subset of the vendor-identified covert channel avenues to determine if such channels are exploitable.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing covert channel analysis; information system design documentation; information system configuration settings and associated documentation; list of vendor-identified covert channel avenues or exploits; covert channel analysis documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with covert channel analysis responsibilities; information system developers/integrators]. **Test**: [*SELECT FROM:* Covert channel avenues to determine if such channels are exploitable].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-32	**INFORMATION SYSTEM PARTITIONING**
SC-32.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system physical domains (or environments); information system facility diagrams; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel installing, configuring, and/or maintaining the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-33	**TRANSMISSION PREPARATION INTEGRITY**
SC-33.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system in preparation for transmission protects the integrity of information during the processes of:* – *data aggregation;* – *packaging; and* – *transformation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Transmission integrity capability within the information system].

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

ASSESSMENT PROCEDURE	
SC-34	**NON-MODIFIABLE EXECUTABLE PROGRAMS**
SC-34.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the applications that are to be loaded and executed from hardware-enforced, read-only media;* *(ii) the organization defines the information system components for which the operating environment and organization-defined applications are loaded and executed from hardware-enforced, read-only media; and* *(iii) the information system, at organization-defined information system components, loads and executes:* - *the operating environment from hardware-enforced, read-only media; and* - *organization-defined applications from hardware-enforced, read-only media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of operating system components to be loaded from hardware-enforced, read-only media; list of applications to be loaded from hardware-enforced, read-only media; media used to load and execute information system operating environment; media used to load and execute information system applications; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel installing, configuring, and/or maintaining the information system].

SC-34(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS
SC-34(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the information system components to be employed with no writeable storage; and* *(ii) the organization employs organization-defined information system components with no writeable storage that are persistent across component restart or power on/off.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system components to be employed without writeable storage capability; other relevant documents or records].

SC-34(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS
SC-34(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects the integrity of the information on read-only media.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing protection of information on read-only media; information system design documentation; information system configuration settings and associated documentation; information system architecture; other relevant documents or records]. **Test**: [*SELECT FROM:* Organizational capability for protecting information integrity on read-only media].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-1	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**
SI-1.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops and formally documents system and information integrity policy;* *(ii) the organization system and information integrity policy addresses:* - *purpose;* - *scope;* - *roles and responsibilities;* - *management commitment;* - *coordination among organizational entities; and* - *compliance;* *(iii) the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities;* *(iv) the organization develops and formally documents system and information integrity procedures;* *(v) the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls; and* *(vi) the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and information integrity responsibilities].
SI-1.2	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of system and information integrity policy reviews/updates;* *(ii) the organization reviews/updates system and information integrity policy in accordance with organization-defined frequency;* *(iii) the organization defines the frequency of system and information integrity procedure reviews/updates; and* *(iv) the organization reviews/updates system and information integrity procedures in accordance with organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with system and information integrity responsibilities].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-2	**FLAW REMEDIATION**
SI-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies, reports, and corrects information system flaws;* *(ii) the organization tests software updates related to flaw remediation for effectiveness before installation;* *(iii) the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation; and* *(iv) the organization incorporates flaw remediation into the organizational configuration management process.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with flaw remediation responsibilities].

SI-2(1)	**FLAW REMEDIATION**
SI-2(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization centrally manages the flaw remediation process; and* *(ii) the organization installs software updates automatically.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting centralized management of flaw remediation and automatic software updates].

SI-2(2)	FLAW REMEDIATION
SI-2(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation; and* *(ii) the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information system flaw remediation update status].

SI-2(3)	FLAW REMEDIATION
SI-2(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the benchmarks to which the organization's measurement of time elapsed between flaw identification and flaw remediation should be compared;* *(ii) the organization measures the time between flaw identification and flaw remediation; and* *(iii) the organization compares the time measured between flaw identification and flaw remediation with organization-defined benchmarks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records].

SI-2(4)	FLAW REMEDIATION
SI-2(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system components for which automated patch management tools are to be employed to facilitate flaw remediation; and* *(ii) the organization employs automated patch management tools to facilitate flaw remediation to organization-defined information system components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms facilitating flaw remediation to information system components].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-3	**MALICIOUS CODE PROTECTION**
SI-3.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:* - *transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or* - *inserted through the exploitation of information system vulnerabilities;* *(ii) the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:* - *transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; or* - *inserted through the exploitation of information system vulnerabilities;* *(iii) the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;* *(iv) the organization defines the frequency of periodic scans of the information system by malicious code protection mechanisms;* *(v) the organization defines one or more of the following actions to be taken in response to malicious code detection:* - *block malicious code;* - *quarantine malicious code; and/or* - *send alert to administrator;* *(vi) the organization configures malicious code protection mechanisms to:* - *perform periodic scans of the information system in accordance with organization-defined frequency;* - *perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and* - *take organization-defined action(s) in response to malicious code detection; and* *(vii) the organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with malicious code protection responsibilities]. **Test:** [*SELECT FROM:* Automated mechanisms implementing malicious code protection capability].

SI-3(1)	MALICIOUS CODE PROTECTION
SI-3(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages malicious code protection mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].

SI-3(2)	MALICIOUS CODE PROTECTION
SI-3(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system automatically updates malicious code protection mechanisms, including signature definitions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records].

SI-3(3)	MALICIOUS CODE PROTECTION
SI-3(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents non-privileged users from circumventing malicious code protection capabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing malicious code protection capability].

SI-3(4)	MALICIOUS CODE PROTECTION
SI-3(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system updates malicious code protection mechanisms only when directed by a privileged user.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing malicious code protection capability].

SI-3(5)	MALICIOUS CODE PROTECTION
SI-3(5).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization does not allow users to introduce removable media into the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with malicious code protection responsibilities].

SI-3(6)	MALICIOUS CODE PROTECTION
SI-3(6).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of testing malicious code protection mechanisms; and* *(ii) the organization tests malicious code protection mechanisms, in accordance with organization-defined frequency, by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing malicious code protection capability].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-4	**INFORMATION SYSTEM MONITORING**
SI-4.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines objectives for monitoring events on the information system;* *(ii) the organization monitors events on the information system in accordance with organization-defined objectives and detects information system attacks;* *(iii) the organization identifies unauthorized use of the information system;* *(iv) the organization deploys monitoring devices:* - *strategically within the information system to collect organization-determined essential information; and* - *at ad hoc locations within the system to track specific types of transactions of interest to the organization;* *(v) the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and* *(vi) the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

SI-4(1)	**INFORMATION SYSTEM MONITORING**
SI-4(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system-wide intrusion detection capability].

SI-4(2)	INFORMATION SYSTEM MONITORING
SI-4(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools to support near real-time analysis of events.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated tools supporting near real-time event analysis].

SI-4(3)	INFORMATION SYSTEM MONITORING
SI-4(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms].

SI-4(4)	INFORMATION SYSTEM MONITORING
SI-4(4).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms].

SI-4(5)	INFORMATION SYSTEM MONITORING
SI-4(5).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines indicators of compromise or potential compromise to the security of the information system; and* *(ii) the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system monitoring real-time alert capability].

SI-4(6)	INFORMATION SYSTEM MONITORING
SI-4(6).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system-wide intrusion detection and prevention capability].

SI-4(7)	INFORMATION SYSTEM MONITORING
SI-4(7).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines incident response personnel (identified by name and/or by role) to be notified of suspicious events;* *(ii) the organization defines least-disruptive actions to be taken by the information system to terminate suspicious events;* *(iii) the information system notifies organization-defined incident response personnel of suspicious events; and* *(iv) the information system takes organization-defined least-disruptive actions to terminate suspicious events.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system notification capability].

SI-4(8)	INFORMATION SYSTEM MONITORING
SI-4(8).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization protects information obtained from intrusion-monitoring tools from:* – *unauthorized access;* – *modification; and* – *deletion.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

SI-4(9)	INFORMATION SYSTEM MONITORING
SI-4(9).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for testing/exercising intrusion-monitoring tools; and* *(ii) the organization tests/exercises intrusion-monitoring tools in accordance with organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; documentation providing evidence of testing intrusion monitoring tools; other relevant documents or records].

SI-4(10)	INFORMATION SYSTEM MONITORING
SI-4(10).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization makes provisions so that encrypted traffic is visible to information system monitoring tools.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records].

SI-4(11)	INFORMATION SYSTEM MONITORING
SI-4(11).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization to discover anomalies analyzes outbound communications traffic at:* – *the external boundary of the system (i.e., system perimeter); and* – *as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system monitoring logs or records; other relevant documents or records].

SI-4(12)	INFORMATION SYSTEM MONITORING
SI-4(12).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines inappropriate or unusual activities with security implications that should trigger alerts to security personnel; and* *(ii) the organization employs automated mechanisms to alert security personnel of the organization-defined inappropriate or unusual activities with security implications.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; list of inappropriate or unusual activities that trigger alerts; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing alerts to security personnel for inappropriate or unusual activities].

SI-4(13)	INFORMATION SYSTEM MONITORING
SI-4(13).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization analyzes communications traffic/event patterns for the information system;* *(ii) the organization develops profiles representing common traffic patterns and/or events;* *(iii) the organization defines the respective measurements to which the organization must tune system monitoring devices to reduce the number of false positives and false negatives; and* *(iv) the organization uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and false negatives to their respective organization-defined measures.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; list of common traffic patterns and/or events; information system protocols documentation; list of acceptable thresholds for false positives and false negatives; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

SI-4(14)	INFORMATION SYSTEM MONITORING
SI-4(14).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs a wireless intrusion detection system to:* – *identify rogue wireless devices to the information system;* – *detect attack attempts to the information system; and* – *detect potential compromises/breaches to the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing wireless communications intrusion detection capability].

SI-4(15)	INFORMATION SYSTEM MONITORING
SI-4(15).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing wireless communications intrusion detection capability].

SI-4(16)	INFORMATION SYSTEM MONITORING
SI-4(16).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; event correlation logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

SI-4(17)	INFORMATION SYSTEM MONITORING
SI-4(17).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization correlates results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; event correlation logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system monitoring responsibilities].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-5	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**
SI-5.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;* *(ii) the organization generates internal security alerts, advisories, and directives;* *(iii) the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;* *(iv) the organization disseminates security alerts, advisories, and directives to organization-identified personnel; and* *(v) the organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system].

SI-5(1)	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**
SI-5(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing the distribution of security alert and advisory information].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-6	**SECURITY FUNCTIONALITY VERIFICATION**
SI-6.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the appropriate conditions, including the system transitional states if applicable, for verifying the correct operation of security functions;* *(ii) the organization defines for periodic security function verification, the frequency of the verifications;* *(iii) the organization defines information system responses and alternative action(s) to anomalies discovered during security function verification;* *(iv) the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and* *(v) the information system responds to security function anomalies in accordance with organization-defined responses and alternative action(s).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Security function verification capability].

SI-6(1)	SECURITY FUNCTIONALITY VERIFICATION
SI-6(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides notification of failed automated security tests.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; automated security test results; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing alerts and/or notifications for failed automated security tests].

SI-6(2)	SECURITY FUNCTIONALITY VERIFICATION
SI-6(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system provides automated support for the management of distributed security testing.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms supporting the management of distributed security function testing].

SI-6(3)	SECURITY FUNCTIONALITY VERIFICATION
SI-6(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization identifies organizational officials with information security responsibilities designated to receive the results of security function verification; and* *(ii) the organization reports the results of security function verification to designated organizational officials with information security responsibilities.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security functionality verification responsibilities; organizational personnel with information security responsibilities].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-7	**SOFTWARE AND INFORMATION INTEGRITY**
SI-7.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system detects unauthorized changes to software and information.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Software integrity protection and verification capability].

SI-7(1)	**SOFTWARE AND INFORMATION INTEGRITY**
SI-7(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the frequency of integrity scans to be performed on the information system; and* *(ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records].

SI-7(2)	**SOFTWARE AND INFORMATION INTEGRITY**
SI-7(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records].

SI-7(3)	SOFTWARE AND INFORMATION INTEGRITY
SI-7(3).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization employs centrally managed integrity verification tools.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records].

SI-7(4)	SOFTWARE AND INFORMATION INTEGRITY
SI-7(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system components that require use of tamper-evident packaging;* *(ii) the organization defines the conditions (i.e., transportation from vendor to operational site, during operation, both) under which tamper-evident packaging must be used for organization-defined information system components; and* *(iii) the organization requires use of tamper-evident packaging for organization-defined information system components during organization-defined conditions.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing software and information integrity; information system component packaging; other relevant documents or records].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-8	**SPAM PROTECTION**
SI-8.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means;* *(ii) the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, removable media, or other common means; and* *(iii) the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with spam protection responsibilities]. **Test**: [*SELECT FROM:* Automated mechanisms implementing spam detection and handling capability].

SI-8(1)	SPAM PROTECTION
SI-8(1).1	**ASSESSMENT OBJECTIVE:** *Determine if the organization centrally manages spam protection mechanisms.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records].

SI-8(2)	SPAM PROTECTION
SI-8(2).1	**ASSESSMENT OBJECTIVE:** *Determine if the information system automatically updates spam protection mechanisms (including signature definitions).* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-9	**INFORMATION INPUT RESTRICTIONS**
SI-9.1	**ASSESSMENT OBJECTIVE:** *Determine if the organization restricts the capability to input information to the information system to authorized personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for implementing restrictions on individual authorizations to input information into the information system].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-10	**INFORMATION INPUT VALIDATION**
SI-10.1	**ASSESSMENT OBJECTIVE:** *Determine if the information system checks the validity of information inputs.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify validity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system capability for checking validity of information inputs].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-11	**ERROR HANDLING**
SI-11.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the information system identifies potentially security-relevant error conditions;* *(ii) the organization defines sensitive or potentially harmful information that should not be contained in error logs and administrative messages;* *(iii) the information system generates error messages that provide information necessary for corrective actions without revealing organization-defined sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries; and* *(iv) the information system reveals error messages only to authorized personnel.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test:** [*SELECT FROM:* Information system error handling capability].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-12	**INFORMATION OUTPUT HANDLING AND RETENTION**
SI-12.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and* *(ii) the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information output handling and retention responsibilities].

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

ASSESSMENT PROCEDURE	
SI-13	**PREDICTABLE FAILURE PREVENTION**
SI-13.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines information system components for which mean time to failure rates should be considered to protect the information system from harm;* *(ii) the organization protects the information system from harm by considering mean time to failure rates for organization-defined information system components in specific environments of operation;* *(iii) the organization provides substitute information system components, when needed; and* *(iv) the organization provides a mechanism to exchange active and standby roles of the components.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with predictable failure prevention responsibilities].

SI-13(1)	PREDICTABLE FAILURE PREVENTION
SI-13(1).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the maximum fraction or percentage of mean time to failure in order to transfer the responsibilities of an information system component that is out of service to a substitute component; and* *(ii) the organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than the organization-defined fraction or percentage of mean time to failure.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organization personnel with predictable failure prevention responsibilities].

SI-13(2)	PREDICTABLE FAILURE PREVENTION
SI-13(2).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period that a process is allowed to execute without supervision; and* *(ii) the organization does not allow a process to execute without supervision for more than the organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system predictable failure prevention capability].

SI-13(3)	PREDICTABLE FAILURE PREVENTION
SI-13(3).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the minimum frequency with which the organization manually initiates a transfer between active and standby information system components if the mean time to failure exceeds the organization-defined time period;* *(ii) the organization defines the time period that the mean time to failure must exceed before the organization manually initiates a transfer between active and standby information system components; and* *(iii) the organization manually initiates a transfer between active and standby information system components at least once per the organization-defined frequency if the mean time to failure exceeds the organization-defined time period.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. **Interview:** [*SELECT FROM:* Organizational personnel with predictable failure prevention responsibilities]. **Test**: [*SELECT FROM:* Information system predictable failure prevention capability].

SI-13(4)	PREDICTABLE FAILURE PREVENTION
SI-13(4).1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization defines the time period for a standby information system component to successfully and transparently assume the role of an information system component that has failed;* *(ii) the organization defines the organization-defined alarm when an information system component failure is detected; and* *(iii) the organization, if an information system component failure is detected:* - *ensures that the standby information system component successfully and transparently assumes its role within the organization-defined time period; and* - *activates the organization-defined alarm and/or automatically shuts down the information system.* **POTENTIAL ASSESSMENT METHODS AND OBJECTS:** **Examine**: [*SELECT FROM:* System and information integrity policy; procedures addressing predictable failure prevention; information system design documentation; information system configuration settings and associated documentation; list of actions to be taken once information system component failure is detected; other relevant documents or records]. **Test**: [*SELECT FROM:* Information system predictable failure prevention capability].

APPENDIX G

SECURITY ASSESSMENT REPORTS

DOCUMENTING THE FINDINGS FROM SECURITY CONTROL ASSESSMENTS

The primary purpose of the *security assessment report* is to convey the results of the security assessment to appropriate organizational officials. The security assessment report is included in the security authorization package along with the security plan (including an updated risk assessment), and the plan of action and milestones to provide authorizing officials with the information necessary to make credible, risk-based decisions on whether to place an information system into operation or continue its operation. As the security assessment and authorization process becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process as an integrated and tightly coupled part of the system development life cycle, the ability to update the security assessment report frequently becomes a critical aspect of an information security program.

It is important to emphasize the relationship, described in Special Publication 800-37, among the three key documents in the authorization package (i.e., the security plan, the security assessment report, and the plan of action and milestones). It is these documents that provide the most reliable indication of the overall security state of the information system and the ability of the system to protect to the degree necessary, the organization's operations and assets, individuals, other organizations, and the Nation. Updates to these key documents are provided on an ongoing basis in accordance with the continuous monitoring program established by the organization.

The security assessment report provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any weaknesses or deficiencies in the security controls.[51] This appendix provides a template for reporting the results from security control assessments. Organizations are not restricted to the specific template format; however, it is anticipated that the overall report of an assessment will include similar information to that detailed in the template for each security control assessed, preceded by a summary providing the list of all security controls assessed and the overall status of each control.

Key Elements for Assessment Reporting

The following elements are included in security assessment reports:[52]

- Information system name;
- Security categorization;
- Site(s) assessed and assessment date(s);
- Assessor's name/identification;
- Previous assessment results (if reused);

[51] While the rationale for each determination made is a part of the formal *Security Assessment Report*, the complete set of records produced as a part of the assessment is likely not included in the report. However, organizations retain the portion of these records necessary for maintaining an audit trail of assessment evidence, facilitating reuse of evidence as appropriate, and promoting repeatability of assessor actions.

[52] Information available in other key organizational documents (e.g., security plan, risk assessment, plan of action and milestones, or security assessment plan) need not be duplicated in the security assessment report.

- Security control or control enhancement designator;
- Selected assessment methods and objects;
- Depth and coverage attributes values;
- Assessment finding summary (indicating satisfied or other than satisfied);
- Assessor comments (weaknesses or deficiencies noted); and
- Assessor recommendations (priorities, remediation, corrective actions, or improvements).

The Assessment Findings

Each determination statement executed by an assessor results in one of the following findings: (i) satisfied (S); or (ii) other than satisfied (O). Consider the following example for security control CP-2. The assessment procedure for CP-2 consists of two assessment objectives denoted CP-2.1 and CP-2.2. The assessor initially executes CP-2.1 and produces the following findings:

CP-2.1	**ASSESSMENT OBJECTIVE:** *Determine if:* *(i) the organization develops a contingency plan for the information system that:* - *identifies essential missions and business functions and associated contingency requirements;* **(S)** - *provides recovery objectives, restoration priorities, and metrics;* **(S)** - *addresses contingency roles, responsibilities, assigned individuals with contact information;* **(O)** - *addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;* **(S)** - *addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;* **(S)** *and* - *is reviewed and approved by designated officials within the organization;* **(O)** *(ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;* **(O)** *and* *(iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.* **(O)** **Comments and Recommendations:** CP-2.1 (i) is marked as *other than satisfied* because the contingency plan prepared by the organization did not assign individuals to contingency roles and provide contact information. There was also no evidence that the contingency plan had been reviewed and approved by designated organizational officials. CP-2.1 (iii) is marked as *other than satisfied* because the organization had not distributed copies of the contingency plan to key contingency personnel and organizational elements critical to executing the plan.

In a similar manner, the assessor executes CP-2.2 and produces appropriate findings. During an actual security control assessment, the assessment findings, comments, and recommendations are documented on a Security Assessment Reporting Form. Organizations are encouraged to develop standard templates for reporting that contain the key elements for assessment reporting described above. Whenever possible, automation is used to make assessment data collection and reporting cost-effective, timely, and efficient.

FTC-0002734

APPENDIX H

ASSESSMENT CASES

WORKED EXAMPLES OF ASSESSOR ACTIONS DERIVED FROM ASSESSMENT PROCEDURES

To provide assessors with additional tools and techniques for implementing the assessment procedures in Appendix F, NIST initiated the *Assessment Case Development Project*.[53] The purpose of the project is fourfold: (i) to actively engage experienced assessors from multiple organizations in recommending *assessment cases* that describe specific assessor actions to implement the assessment procedures in Appendix F; (ii) to provide organizations and the assessors supporting those organizations with an exemplary set of assessment cases for each assessment procedure in Appendix F; (iii) to provide a vehicle for ongoing community-wide review of the assessment cases to promote continuous improvement in the security control assessment process for more consistent, effective, and cost-effective security assessments of federal information systems; and (iv) to serve as a basis for reciprocity among various communities of interest. The assessment case development process is described in this appendix and several examples of assessment cases are provided.

Assessment Case Description and Template

The concept of assessment cases emerged during the development process of Special Publication 800-53A. Some organizations prefer the flexibility offered by the generalized assessment procedures in Appendix F, with the opportunity to tailor the procedures for specific organizational requirements and operational environments and to create specific assessor actions and activities for a particular security assessment. Other organizations prefer a more prescriptive approach and desire, to the greatest extent possible, a predefined set of specific assessor actions and activities needed to successfully carry out a security assessment. To facilitate the specificity of the latter approach while maintaining the flexibility of the former approach, assessment cases have been developed for all assessment procedures in Appendix F of this document.

An assessment case represents a worked example of an assessment procedure, identifying the specific actions that an assessor might carry out during the assessment of a security control or control enhancement in an information system. There is one assessment case per control, covering all assessment objectives from the assessment procedure in Appendix F for that control (both base control and all enhancements). The assessment case provides an example by experienced assessors of a potential set of specific assessor action steps to accomplish the assessment that were developed with consideration for the list of potential assessment methods and objects, and incorporating the level of coverage and depth to be applied and the specific purpose to be achieved by each assessor action. This additional level of detail in the assessment cases provides assessors with more prescriptive assessment information. Yet, while being more prescriptive, the assessment cases are not intended to restrict assessor flexibility provided as part of the design principles in Special Publication 800-53A. The assessor remains responsible for making the specified determinations and for providing adequate rationale for the determinations made.

[53] NIST initiated the *Assessment Case Development Project* in October 2007 in cooperation with the Departments of Justice, Energy, Transportation, and the Intelligence Community. The interagency task force developed a full suite of assessment cases based on the assessment procedures provided in Special Publication 800-53A. The assessment cases are available to all public and private sector organizations and can be downloaded from the NIST web site at http://csrc.nist.gov/sec-cert.

The following template is used to create the specific assessment cases for the assessment procedures in Appendix F.

ASSESSMENT CASE	
AA-N	**Security Control Name**
ASSESSMENT – Base Control, Part 1 of x (where x is the number of assessment objectives)	
Assessment Information from Special Publication 800-53A	
This section contains the *determinations* and *potential assessment methods and objects* from Special Publication 800-53A, with a separate row for each unique determination. The numbering in the column to the left associates a unique number with each specific determination. This numbering is used to link the assessor action steps below to the determinations.	
AA-N.1	*Determine if:*
AA-N.1.1	*(i) <determination statement 1>.*
⋮	⋮
AA-N.1.n	*(n) <determination statement n>.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine:** [*ASSIGN ATTRIBUTE VALUES*: <depth>, <coverage>]. [*SELECT FROM*: <object-list>]. **Interview:** [*ASSIGN ATTRIBUTE VALUES*: <depth>, <coverage>]. [*SELECT FROM*: <object-list>]. **Test:** [*ASSIGN ATTRIBUTE VALUES*: <depth>, <coverage>]. [*SELECT FROM*: <object-list>].
Additional Assessment Case Information	
This section contains the additional information provided by the assessment case to help the assessor in planning and conducting the security control assessment.	
	POTENTIAL ASSESSMENT SEQUENCING: PRECURSOR CONTROLS: <security-control-list> CONCURRENT CONTROLS: <security-control-list> SUCCESSOR CONTROLS: <security-control-list>
	This section provides some initial suggestions with regard to sequencing of assessor actions for greater efficiency. *Precursor controls* are those controls whose assessment is likely to provide information either assisting in, or required for, the assessment of this control. *Concurrent controls* are those controls whose assessment is likely to require the assessor to assess similar objects and hence, the assessor may be able to obtain evidence for multiple control assessments at the same time. *Successor controls* are those controls whose assessment will likely need, or benefit from, information obtained from the assessment of this control.
Action Step	**Potential Assessor Evidence Gathering Actions**
Each step is numbered to align with a specific determination statement above.	Suggested assessor action (**Examine**, **Interview**, or **Test**) is identified, along with a likely set of objects to which that action would be applied. As the title of this column indicates, each action step does not necessarily result in a determination. Rather collectively, the set of assessor action steps aligned with a specific determination above provide the evidence necessary to make that determination.
AA-N.1.1.1	[<Assessment Method with assigned depth and coverage attribute values> <Assessment Object(s)>]
⋮	⋮
AA-N.1.1.m	[<Assessment Method with assigned depth and coverage attribute values> <Assessment Object(s)>]
Legend **AA:** Alphanumeric characters representing security control family in Special Publication 800-53. **N:** Numeric character representing the security control number within the family of controls. **n:** Number of determination statements in the assessment object. **m:** Number of action steps associated with a specific determination statement.	

Cautionary Note

The assessment cases developed for this project are not the ***only*** acceptable assessment cases; rather, the cases represent one possible set of assessor actions for organizations (and assessors supporting those organizations) to use in helping to determine the effectiveness of the security controls employed within the information systems undergoing assessments. The following assessment procedure for security control AC-3, illustrates how assessment cases are developed from the template on the preceding page. The assessment cases and any ongoing updates to the cases, will be published regularly on the FISMA Implementation Project Web site at http://csrc.nist.gov/sec-cert.

ASSESSMENT CASE EXAMPLE

ASSESSMENT CASE	
MP-2	**Media Access**
ASSESSMENT – Base Control	
Assessment Information from Special Publication 800-53A	
	ASSESSMENT OBJECTIVE:
MP-2.1	*Determine if:*
MP-2.1.1 **MP-2.1.1a** **MP-2.1.1b** **MP-2.1.1c**	*(i) the organization defines:* - *digital and non-digital media requiring restricted access;* - *individuals authorized to access the media; and* - *security measures taken to restrict access.*
MP-2.1.2	*(ii) the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system media protection responsibilities].
Additional Assessment Case Information	
	POTENTIAL ASSESSMENT SEQUENCING: PRECURSOR CONTROLS: MP-3, MP-4, MP-5, MP-6. CONCURRENT CONTROLS: AC-2, AC-3, AC-19, AU-2, AU-3, CM-6, MP-6, PE-2, PE-3, PE-7, PE-8. SUCCESSOR CONTROLS: NONE.
	General notes to assessor for MP-2: The focus of this control is the organization restricting access to information system media, and not whether the media is allowed to be used (which is covered under AC-19). As indicated in the supplemental guidance for this control, this control addresses both digital and non-digital media.
Action Step	**Potential Assessor Evidence Gathering Actions**
MP-2.1.1a.1	**Examine** information system media protection policy and procedures, access control policy and procedures, physical and environmental protection policy and procedures, or other relevant documents (e.g., system security plan) reviewing for what the organization has defined as the digital and non-digital media requiring restricted access.
MP-2.1.1b.1	**Examine** information system media protection policy and procedures, access control policy and procedures, physical and environmental protection policy and procedures, or other relevant documents (e.g., system security plan) reviewing for what the organization has defined as individuals authorized to access the media identified in MP-2.1.1a.1.
MP-2.1.1c.1	**Examine** information system media protection policy and procedures, access control policy and procedures, physical and environmental protection policy and procedures, or other relevant documents (e.g., system security plan) reviewing for what the organization has defined as measures to be taken for the access of media identified in MP-2.1.1a.1.

ASSESSMENT CASE	
MP-2.1.2.1	**Examine** an agreed-upon representative sample of media access control records or other relevant records for an agreed-upon representative sample of information system media types identified in MP-2.1.1a.1; reviewing for evidence that the measures identified in MP-2.1.1c.1 are implemented as intended.
MP-2.1.2.2	**Examine** an agreed-upon representative sample of operations at media storage facilities and other relevant areas; observing for indication that the measures identified in MP-2.1.1c.1 are implemented as intended.
MP-2.1.2.3	**Examine** an agreed-upon representative sample of operations at media storage facilities and other relevant areas; inspecting for indication that the measures identified in MP-2.1.c.1 are implemented as intended.
MP-2.1.2.4	**Interview** an agreed-upon representative sample of organizational personnel identified in MP-2.1.1b.1 with information system media protection responsibilities; conducting focused discussions for further evidence that the measures identified in MP-2.1.1c.1 are implemented as intended. *Note to assessor:* To facilitate testing of this control, there should be an identified list of storage areas (e.g., identified in the security plan) where the system intends to apply the MP-2 control, and it is assumed that such designated storage areas that either house large concentrations of information system media (e.g., server rooms, communication centers) or house particularly important media with regard to potential impacts if not adequately protected.
ASSESSMENT – Control Enhancement 1	
Assessment Information from Special Publication 800-53A	
	ASSESSMENT OBJECTIVE:
MP-2(1).1	*Determine if:*
MP-2(1).1.1	*(i) the organization employs automated mechanisms to restrict access to media storage areas; and*
MP-2(1).1.2	*(ii) the organization employs automated mechanisms to audit access attempts and access granted to media storage areas.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records]. **Test**: [*SELECT FROM:* Automated mechanisms implementing access restrictions to media storage areas].
Additional Assessment Case Information	
	POTENTIAL ASSESSMENT SEQUENCING: PRECURSOR CONTROLS: MP-3, MP-4, MP-5, MP-6. CONCURRENT CONTROLS: AC-2, AC-3, AC-19, AU-2, AU-3, CM-6, MP-6, PE-2, PE-3, PE-7, PE-8. SUCCESSOR CONTROLS: NONE.
Action Step	Potential Assessor Evidence Gathering Actions
MP-2(1).1.1.1	**Examine** information system media protection policy and procedures, access control policy and procedures, physical and environmental protection policy and procedures, security plan, or other relevant documents; reviewing for the automated mechanisms and configuration settings to be employed to restrict access to designated media storage areas.

ASSESSMENT CASE	
MP-2(1).1.1.2	**Examine** documentation describing the current configuration settings for an agreed-upon specific sample of automated mechanisms identified in MP-2(1).1.1.1; reviewing for indication that the mechanisms are configured as identified in MP-2(1).1.1.1.
MP-2(1).1.1.3	**Examine** an agreed-upon specific sample of media storage facilities; observing for indication that the mechanisms identified in MP-2(1).1.1.1 are implemented as intended.
MP-2(1).1.1.4	**Examine** an agreed-upon specific sample of media storage facilities; inspecting for indication that the mechanisms identified in MP-2(1).1.1.1 are implemented as intended.
MP-2(1).1.1.5	**Test** an agreed-upon specific sample of automated mechanisms identified in MP-2(1).1.1.1; conducting focused testing for evidence that the mechanisms operate as intended.
MP-2(1).1.2.1	**Examine** information system media protection policy and procedures, audit and accountability policy and procedures, physical and environmental protection policy and procedures, security plan, or other relevant documents; reviewing for the automated mechanisms and configuration settings to be employed to audit access attempts and access granted to media access areas.
MP-2(1).1.2.2	**Examine** documentation describing the current configuration settings for an agreed-upon specific sample of automated mechanisms identified in MP-2(1)1.2.1; reviewing for indication that the mechanisms are configured as identified in MP-2(1).1.2.1. *Note to assessor:* Consideration for selecting the specific sample include: selected audit and accountability policies (access attempts/access granted), how many media storage areas should be included in the sample, and how many instances of access attempts are to be examined.
MP-2(1).1.2.3	**Test** an agreed-upon specific sample of automated mechanisms identified in MP-2(1).1.2.1; conducting focused testing for evidence that the mechanisms operate as intended. *Note to assessor:* See note for MP-2(1).1.2.2 above.
ASSESSMENT – Control Enhancement 2	
Assessment Information from Special Publication 800-53A	
	ASSESSMENT OBJECTIVE:
MP-2(2).1	*Determine if the information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Information system media protection policy; procedures addressing media access; other relevant documents or records]. **Test**: [*SELECT FROM:* Cryptographic mechanisms protecting and restricting access to information system information on portable digital media].
Additional Assessment Case Information	
	POTENTIAL ASSESSMENT SEQUENCING: PRECURSOR CONTROLS: NONE. CONCURRENT CONTROLS: NONE. SUCCESSOR CONTROLS: NONE.
Action Step	**Potential Assessor Evidence Gathering Actions**
MP-2(2).1.1.1	**Examine** information system media protection policy and procedures, audit and accountability policy and procedures, physical and environmental protection policy and procedures, security plan, or other relevant documents; reviewing for required use of the cryptographic mechanisms and the configuration settings to be employed to protect and restrict access to information on portable digital media.

ASSESSMENT CASE	
MP-2(2).1.1.2	**Examine** documentation describing the current configuration settings for an agreed-upon specific sample of automated mechanisms identified in MP-2(1)1.2.1; reviewing for indication that the mechanisms are configured as identified in MP-2(2).1.1.1. *Note to assessor:* Consideration for selecting the specific sample include: selected audit and accountability policies (access attempts/access granted), how many media storage areas should be included in the sample, and how many instances of access attempts are to be examined.
MP-2(2).1.1.3	**Test** an agreed-upon specific sample of automated mechanisms identified in MP-2(2).1.1.2; conducting focused testing for evidence that the mechanisms operate as intended. *Note to assessor:* See note for MP-2(2).1.1.2 above.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 9
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 10
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 11
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 12
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 13
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

FTC has submitted 'Cole Att 13 (Lifelock-0135783) (REDACTED).Csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

FTC has submitted 'Cole Att 13 (Lifelock-0135784) (REDACTED).Csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

FTC has submitted 'Cole Att 13 (Lifelock-0135785) (REDACTED).Csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

FTC has submitted 'Cole Att 13 (Lifelock-0135786) (REDACTED).Csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

FTC has submitted 'Cole Att 13 (Lifelock-0138077) (REDACTED).Csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

FTC has submitted 'Cole Att 13 (Lifelock-0138078) (REDACTED).Csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 14
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 15
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 16
TO EXPERT REPORT OF DR. ERIC B. COLE

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 17
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 18
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

Welcome to the new JIRA !

www LifeLock Web Dev / WWW-659

XSS Problem in Jobs Site

Agile Board | More Actions | Views

Details

Type:	Bug	Status:	Resolved
Priority:	Minor	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	WWW_20120830
Component/s:	Scripting		
Labels:	None		

Description

https://www.lifelock.jobs/job-openings/apply/?refid=605a07db%22%3E%3Cscript%3Ealert%281%29%3C/script%3E94cee881741&title=Contract+QA+SME
https://www.lifelock.jobs/job-openings/apply/?refid=605&title=Contract+QA+SMEc04c7%22%3E%3Cscript%3Ealert%28%27XSS%27%29%3C/script%3E837d07855a0

People

Assignee:	cdrummond
Reporter:	cdrummond

Vote (0) Watch (0)

Dates

Created:	30/Aug/12 10:11 AM
Updated:	30/Aug/12 12:14 PM
Resolved:	30/Aug/12 12:14 PM

LIFELOCK-0132479

Agile

Support Engineering / SEP-288

Vulnerability Fix - Disable AutoComplete

Edit | Assign | Comment | More Actions | Start Progress | Resolve Issue | Workflow

Details

Type:	Story	Status:	Open
Priority:	Critical	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	Backlog
Component/s:	Security		
Labels:	None		

Description

Vulnerability discovered during recent penetration test.

A number of fields that contain sensitive information in Member Portal do not have autocomplete disabled. Consequently, data from these fields may be stored by the web browser.

For each of the fields listed below, please add the AutoComplete="off" attribute. This will keep the browser from caching this sensitive information. Of course, validate these changes with the business, as they affect user experience.

Fields:
User ID on the Reset Password page
Challenge Questions in the Reset Password process
User ID in the Locked User Account Reset process
Username field on the Employee Login page on lifelock.jobs

Support Engineering / SEP-290

Vulnerability Remediation - Cookie Settings

Agile Board | More Actions

Details

Type:	Story	Status:	Open
Priority:	Major	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	Backlog
Component/s:	Security		
Labels:	None		

Description

The LifeLock Portal application does not mark its sensitive cookies as "HttpOnly". This attribute is supported by modern browsers and prevents the cookie from being accessed via JavaScript. Without this configuration, an attacker could hijack user sessions more easily by stealing cookies directly through XSS attacks.
The following sensitive cookies are set without the "HttpOnly" flag:
https://secure.lifelock.com/

Support Engineering / SEP-291

Vulnerability Remediation - HTTP Response Information Disclosure

Agile Board | More Actions

Details

Type:	Story	Status:	Open
Priority:	Major	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	Backlog
Component/s:	Security		
Labels:	None		

Description

This vulnerability was discovered during a recent penetration test. Please work with the Infrastructure team if necessary for Linux or F5 configuration assistance.

The LifeLock web servers reveal information about the software it runs. Headers within HTTP responses contain platform information, including the web server type and version. Attackers can often use this type of information to more effectively target the system.

http://www.lifelock.com/
Server - Apache/2.2.3 (CentOS)
X-Powered-By - PHP/5.3.14

http://www.lifelock.jobs/
Server - Apache/2.2.3 (CentOS)
X-Powered-By - PHP/5.3.14

https://secure.lifelock.com/version/ - HTTP 200 response
JDK 1.6.0_22

http://origin-cdn.lifelock.com/test - HTTP 404 response
Apache 2.2.3

Support Engineering / SEP-292

Vulnerability Remediation - Hidden Directory Enumeration

Agile Board | More Actions

Details

Type:	Story	Status:	Open
Priority:	Critical	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	Backlog
Component/s:	Security		
Labels:	None		

Description

This vulnerability was discovered during a recent penetration test.

The web application exposes the presence of a directory in the site. Although the directory does not list its content, the information may help an attacker to develop further attacks against the site. For example, by knowing the directory name, an attacker can guess its content type and possibly file names that reside in it or sub-directories under it. The more sensitive the content is, the more severe the issue is.

Typically, a hidden directory can be detected when a "403 - Forbidden" response is issued by the web server, but any response that is not "404 - Not Found" can be used to detect the presence of a directory. For example, some web servers issue "courtesy redirects" when the trailing slash of a directory is omitted.
The following hidden directories were detected:
/cgi-bin/
/common/
/scripts/
/images/

If the forbidden resource is not required, remove it from the site. If possible, issue a "404 - Not Found" response status code instead of a "403 - Forbidden" or other responses. This change will obfuscate the presence of the directory in the site and will prevent the site structure from being exposed.

It's unclear which site the tester is referring to with this finding, please check www.lifelock.com, secure.lifelock.com, and lifelock.jobs.

Support Engineering / SEP-293

Vulnerability Remediation - No Clickjacking Protection

Agile Board | More Actions

Details

Type:	Story	Status:	Open
Priority:	Critical	Resolution:	Unresolved
Affects Version/s:	None	Fix Version/s:	Backlog
Component/s:	Security		
Labels:	None		

Description

This vulnerability was discovered during a recent penetration test.

The LifeLock Portal application does not use the available mechanisms to instruct a browser to defend itself against Clickjacking attacks. Clickjacking (aka, "UI redressing") is a technique that tricks users into revealing confidential information or taking an unwanted action while clicking on a seemingly innocuous area of a web page. An IFRAME (inline frame) element is often used in this type of attack.

The "X-Frame-Options" response header is supported by current browsers and specifies that the page should not be loaded within a frame. The following figure is a sample HTTP response from the application showing that the header is not present.
http://secure.lifelock.com/portal/

Add the X-Frame-Options response header to all pages within the application. Possible values for the header are "DENY", which prevents any domain from framing the page, and "SAMEORIGIN", which only allows the same domain to frame the page.
In this case, none of the functionality appeared to use frames, so FishNet Security recommends setting the value to "DENY" as follows:

```
X-Frame-Options: DENY
```

A second step is to use a JavaScript Framekiller. Although this feature can be bypassed in some circumstances, it serves as a useful defense in depth mechanism for older browsers that do not respect the X-Frame-Options headers.

For more information, please see:
https://www.owasp.org/index.php/Clickjacking https://www.owasp.org/index.php/Cross_Frame_Scripting https://developer.mozilla.org/en/The_X-Frame-Options_response_header
http://en.wikipedia.org/wiki/Framekiller

Please evaluate this, as this change may impact the user experience.

LifeLock

September 2012 Penetration Test (WWW, Enrollment, & Member Portal)

Vulnerability Remediation

The penetration test performed against LifeLock (www, Enrollment, & Member Portal) by (b)(3):6(f),(b)(4) in September 2012 resulted in 12 issues, with remediation recommendations. This document outlines LifeLock's intentions regarding the 12 issues raised.

Finding	Remediation Procedure	LifeLock Intention	Remediation Details
1 – XSS on www.lifelock.jobs	Fix input validation and output encoding	Accept Finding and Remediate	Fix went into production on 8-30-12
2 – Weak Password Requirements	Validate finding & evaluate password requirements	Accept Finding and Remediate	False Positive – confirmed by InfoSec that member portal requires 7 characters, one number, one capital, and one symbol
3 – Autocomplete not disabled	Code change to set autocomplete to off	Accept Finding and Remediate	(b)(3):6(f),(b)(4) # 81911 (on-hold for system stability projects)
4 – Sensitive Data Displayed	Evaluate with business masking identified data	Accept Finding and Remediate	PM (Michele Grant) has added masking of DL#, and Bank #, to product enhancement queue.
5 – Improper caching directive	Change cache-control parameter	Accept Finding and Remediate	(b)(3):6(f),(b)(4) # 81913 Completed 11-28-12
6 – insecure cookie	Change secure flag	Accept Finding and Remediate	(b)(3):6(f),(# 81915 (on-hold for system stability projects)
7 – Cookie path not set	Change cookie path	Accept Finding and Remediate	(b)(3):6(f), # 81915 (on-hold for system stability projects)
8 – Cookie not HTTP only	Set HTTP only flag	Accept Finding and Remediate	(b)(3):6(f), # 81915 (on-hold for system stability projects)
9 – HTTP Response disclosure	Remove HTTP headers with platform information	Accept Finding and Remediate	(b)(3):6(f), # 81916 (on-hold for system stability projects)
10 – Directory enumeration	Evaluate if discovered directories are	Accept Finding and Remediate	(b)(3):6(f),(b)(4) # 81926 (on-hold for system stability projects)

	required		
11 – No Clickjacking Protection	Use X-Frame-Options HTTP header	Accept Finding and Remediate	(b)(3):6(f), (b)(4) # 81932 (on-hold for system stability projects)
12 – Robots.txt	Evaluate contents of robot.txt file	Accept Finding and Remediate	Evaluate contents of robot.txt file. Contents evaluated by InfoSec on 11-12-12. No issues found, no remediation is necessary.

LifeLock®

November 2012 Network Penetration Test (b)(3):6 (f),(b)(4)

Vulnerability Remediation

The penetration test performed against LifeLock by (b)(3):6 in November 2012 resulted in 14 issues, with remediation recommendations. This document outlines LifeLock's intentions regarding the 14 issues raised.

Finding	Remediation Procedure	LifeLock Intention	Remediation Details
Perimeter Network Test			
1 – SSL Weak Ciphers	Issue update/strong SSL certificates	Validate Issue & Remediate	Cert for REDACTED adequate (risk accepted) REDACTED is old (b)(3):6(f) VPN. (b)(3):6(f), (b)(4) #83627.
2 – Autocomplete Web Forms	Set autocomplete to off	Validate Issue & Remediate	Accept risk for REDACTED (b)(3):6(f), (b)(4) #81911 (on-hold for system stability projects)
Internal Network Test			
1 – Directory Traversal	Remediate flaw – vendor patch or configuration change	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #83219
2 – Local Admin Password Reuse	Change GPO setting	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #83228
3 – Guessable Password	Change & strengthen passwords	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #83232
4 – Tomcat Version	Update Tomcat	Validate Issue & Remediate	False positive – internal scanning (w/ credentials) finds no issues with tomcat version.
5 – Apache Version	Update Apache	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #81592 (In progress before assessment)
6 – Information Disclosure	Configuration Change	Validate Issue & Remediate	(b)(3):6(f),(b)(4) #83629
7 – SMB Null Sessions	Disable Null Sessions	Validate Issue & Remediate	Risk Accepted

8 – Subversion Information Disclosure	Configuration Change	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #83631 (completed)
9 – SMB Signing	Enable SMB Signing	Validate Issue & Remediate	Risk Accepted (Windows is evaluating the possibility of making this change)
10 – Telnet	Disable Telnet	Validate Issue & Remediate	Risk Accepted – These are VIPs. Covered by our internal scans of the "real" instance.
11 – MS12-070 Patch	Apply Patch	Validate Issue & Remediate	False positive – internal scanning (w/ credentials) does not find this issue with SQL Server
12 – SSL Cert Issues	Update Certs	Validate Issue & Remediate	These interfaces are not for production data use (mostly admin consoles only) – Risk Accepted
13 – SNMP Default String	Change SNMP String	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #81253 #81254 #81256 #81262
14 – RDP Issues	Configuration Change	Validate Issue & Remediate	Risk Accepted (Windows is evaluating the possibility of making this change)

Request ID : 81253 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR[REDACTED] - SNMP community name

By Austin Appel on Oct 24, 2012 04:27 PM Due Date : Oct 30, 2012 04:27 PM

Status : Open
Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Description

Notes(1) Conversations Associate Change

Machine Name and/or IP:
[REDACTED]

Discovery Method & Date:
Internal PCI Scan on Oct 11, 2012

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6(f),(b)(4)

Description & Remediation Info:
Default or Guessable SNMP community name
The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. This community string is a default on a number of SNMP servers.
This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Date completed	-	Remediation Status	Closed - Remediated (to be verified)
Service Category	Not Assigned	InfoSec Recommended Course of Action	Apply Fix - Defined SLA
Group	Information Security	Action Decision	Not Assigned
Technician	Austin Appel	Asset	-
Created By	Austin Appel	Department	Products & Technology
SLA	Low SLA	Template	IT Only - Vulnerability Remediation Request
Created Date	Oct 24, 2012 04:27 PM	DueBy Date	Oct 30, 2012 04:27 PM
Response DueBy Time	-	Last Update Time	Jun 6, 2013 08:39 PM

Requester Details

Edit

Requester Name	Austin Appel	E-mail Address	Austin.Appel@lifelock.com
Contact number	(480) 457-2061	Mobile number	(b)(6),(b)(7)(C)
Department	Products & Technology	Administrator	-
Business Impact	-		

TOP

Discussion Notes

Add Notes

[1 note(s)]

User: (b)(3):6(f),(b)(4)

Private

Public community disabled

Mar 26, 2013 02:54 PM

Request ID : 81254 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR REDACTED) - SNMP community name

By Austin Appel on Oct 24, 2012 04:47 PM Due Date : Oct 30, 2012 04:47 PM

Status : Open
Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Description

Notes(1) Conversations Associate Change

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Internal PCI Scan on Oct 11, 2012

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6(f),(b)(4)

Description & Remediation Info:
Default or Guessable SNMP community name
The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. This community string is a default on a number of SNMP servers.
This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Date of Request	Oct 24, 2012 04:28 PM	**CVE Reference**	CVE-
Date completed	-	**Remediation Status**	Closed - Remediated (to be verified)
Service Category	Not Assigned	**InfoSec Recommended Course of Action**	Apply Fix - Defined SLA
Group	Information Security	**Action Decision**	Not Assigned
Technician	Austin Appel	**Asset**	-
Created By	Austin Appel	**Department**	Products & Technology
SLA	Low SLA	**Template**	IT Only - Vulnerability Remediation Request
Created Date	Oct 24, 2012 04:47 PM	**DueBy Date**	Oct 30, 2012 04:47 PM
Response DueBy Time	-	**Last Update Time**	Jun 6, 2013 08:39 PM

Requester Details

Edit

Requester Name	Austin Appel	**E-mail Address**	Austin.Appel@lifelock.com
Contact number	(480) 457-2061	**Mobile number**	(b)(6),(b)(7)(C)
Department	Products & Technology	**Administrator**	-
Business Impact	-		

TOP

Discussion Notes

Add Notes

[1 note(s)]

LIFELOCK-0132490

User: (b)(3):6(f),(b)(4) **Private** Mar 26, 2013 02:54 PM

Public community disabled

Request ID : 81256 Edit Assign ▼ Actions ▼ Reply ▼

VRR REDACTED) - SNMP community name

By Austin Appel on Oct 24, 2012 04:54 PM Due Date : Oct 30, 2012 04:54 PM

Status : Closed
Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Description

Notes(1) Conversations Associate Change

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Internal PCI Scan on Oct 11, 2012

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6(f),(b)(4)

Description & Remediation Info:
Default or Guessable SNMP community name
The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. This community string is a default on a number of SNMP servers.
This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

ate completed	Mar 25, 2013 04:56 PM	Remediation Status	Closed - Remediated (verified)
ervice Category	Not Assigned	InfoSec Recommended Course of Action	Apply Fix - Defined SLA
roup	Information Security	Action Decision	Not Assigned
echnician	Austin Appel	Asset	-
reated By	Austin Appel	Department	Products & Technology
LA	Low SLA	Template	IT Only - Vulnerability Remediation Request
reated Date	Oct 24, 2012 04:54 PM	DueBy Date	Oct 30, 2012 04:54 PM
ompleted Date	May 15, 2013 04:56 PM	Resolved Date	May 15, 2013 04:56 PM
ime Elapsed	1595hrs 2min	Response DueBy Time	-
equest Closure Code	Not Assigned	Request Closure Comments	-
ast Update Time	Jun 6, 2013 08:24 PM		

equester Details

Edit

equester Name	Austin Appel	E-mail Address	Austin.Appel@lifelock.com
ontact number	(480) 457-2061	Mobile number	(b)(6),(b)(7)(C)
epartment	Products & Technology	Administrator	-
usiness Impact	-		

TOP

iscussion Notes

Add Notes

[1 note(s)]

LIFELOCK-0132492

ser (b)(3):6(f),(b)	Private Disabled snmpd	Mar 25, 2013 11:43 AM

Request ID : 81262 Edit Assign Actions Reply

VRR REDACTED) - SNMP community name

By Austin Appel on Oct 24, 2012 05:02 PM Due Date : Oct 30, 2012 05:02 PM

Status : Closed
Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Description

Notes(1) Conversations Associate Change

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Internal PCI Scan on Oct 11, 2012

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6(f),(b)(4)

Description & Remediation Info:
Default or Guessable SNMP community name
The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. This community string is a default on a number of SNMP servers.
This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Secure the SNMP installation

Date of Request	Oct 24, 2012 04:28 PM	CVE Reference	CVE-
Date completed	Mar 26, 2013 05:36 PM	Remediation Status	Closed - Remediated (verified)
Service Category	Not Assigned	InfoSec Recommended Course of Action	Apply Fix - Defined SLA
Group	Information Security	Action Decision	Not Assigned
Technician	Austin Appel	Asset	-
Created By	Austin Appel	Department	Products & Technology
SLA	Low SLA	Template	IT Only - Vulnerability Remediation Request
Created Date	Oct 24, 2012 05:02 PM	DueBy Date	Oct 30, 2012 05:02 PM
Completed Date	May 15, 2013 05:36 PM	Resolved Date	May 15, 2013 05:36 PM
Time Elapsed	1595hrs 34min	Response DueBy Time	-
Request Closure Code	Not Assigned	Request Closure Comments	-
Last Update Time	Jun 6, 2013 08:24 PM		

Requester Details

Edit

Requester Name	Austin Appel	E-mail Address	Austin.Appel@lifelock.com
Contact number	(480) 457-2061	Mobile number	(b)(6),(b)(7)(C)
Department	Products & Technology	Administrator	-
Business Impact	-		

TOP

Discussion Notes

Add Notes

[1 note(s)]

LIFELOCK-0132494

Use (b)(3):6(f),(b)(4) **Private** Mar 26, 2013 02:53 PM

Public community disabled

Request ID : 81592 Edit Close Assign Actions Reply

VRR REDACTED) OpenSSL & (b)(3):6(f), (b)(4) Updates (low)

By Austin Appel on Oct 29, 2012 02:59 PM Due Date : Nov 2, 2012 02:59 PM

Status : Open
Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Description

Notes(3) Conversations Associate Change

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Internal PCI Scan on Oct 13, 2012

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6(f),(b)(4)

Description & Remediation Info:
(b)(3):6 HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368)
Remotely Exploitable Buffer Overflow in mod_ssl
OpenSSL ASN1 BIO vulnerability (CVE-2012-2110)
OpenSSL Invalid TLS/DTLS record attack (CVE-2012-2333)
(b)(3):6(f HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883)
mod_ssl Directive Mapping Buffer Overflow
OpenSSL memory leak caused by uncleared block cipher padding in SSL 3.0 records (CVE-2011-4576)

Date Completed	-	Remediation Status	Closed - No Action (Risk Accepted)
Service Category	Not Assigned	InfoSec Recommended Course of Action	Apply Fix - Defined SLA
Group	Windows Server Support	Action Decision	Not Assigned
Technician	Not Assigned	Asset	-
Created By	Austin Appel	Department	Products & Technology
SLA	Low SLA	Template	IT Only - Vulnerability Remediation Request
Created Date	Oct 29, 2012 02:59 PM	DueBy Date	Nov 2, 2012 02:59 PM
Response DueBy Time	-	Last Update Time	Jul 1, 2013 03:48 PM

Requester Details

Edit

Requester Name	Austin Appel	E-mail Address	Austin.Appel@lifelock.com
Contact number	(480) 457-2061	Mobile number	(b)(6),(b)(7)(C)
Department	Products & Technology	Administrator	-
Business Impact	-		

TOP

Discussion Notes

Add Notes

[3 note(s)]

User: (b)(3):6(f),(b)(4) **Private** LIFELOCK-01324963 03:48 PM

Sent ticket to netapp about it. Not sure what they can do yet. Case No. 2004401886

Request ID : 81911 Edit Assign ▼ Actions ▼ Reply ▼

Vulnerability Fix - Disable AutoComplete

By Jenner Holden on Nov 5, 2012 10:52 AM Due Date : Nov 8, 2012 10:52 AM

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **May 15, 2013 10:50 AM**

Resolution submitted by (b)(3):6(f),(b)(4)

Edit

moved to (b)

LIFELOCK-0132497

Request ID : 81913 Edit Assign ▼ Actions ▼ Reply ▼

Vulnerability Remediation - Fix Caching Directive

By Jenner Holden on Nov 5, 2012 10:57 AM Due Date : Nov 8, 2012 10:57 AM

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **Nov 28, 2012 08:39 AM**

Resolution submitted by : **Brian Kao**

Edit

Member Portal already has "no-cache" setting enabled, and WWW should be allowed to leverage browser caching since it's a public content based website. Jenner has also agreed to close the ticket.

Request ID : 81915 Edit Assign ▼ Actions ▼ Reply ▼

Vulnerability Remediation - Cookie Settings

By Jenner Holden on Nov 5, 2012 11:03 AM Due Date : N/A

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **May 15, 2013 11:11 AM**

Resolution submitted by : **Kate Rinehart**

Edit

JIRA TICKET EXISTS, THIS IS A DUPLICATE

LIFELOCK-0132499

Request ID : 81916

Edit | Assign ▼ | Actions ▼ | Reply ▼

Vulnerability Remediation - HTTP Response Information Disclosure

By Jenner Holden on Nov 5, 2012 11:16 AM **Due Date** : May 6, 2013 09:59 AM

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **May 15, 2013 11:03 AM**

Resolution submitted by : (b)(3):6(f),(b)(4)

Edit

moved to (b)(3):6(f)

LIFELOCK-0132500

Request ID : 81926 Edit Assign ▼ Actions ▼ Reply ▼

Vulnerability Remediation - Hidden Directory Enumeration

By Jenner Holden on Nov 5, 2012 12:38 PM Due Date : Nov 8, 2012 12:38 PM

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : May 15, 2013 11:06 AM

Resolution submitted by [redacted]

LIFELOCK-0132501 Edit

in [redacted]

Request ID : 81932

Edit | Assign ▼ | Actions ▼ | Reply ▼

Vulnerability Remediation - No Clickjacking Protection

By Jenner Holden on Nov 5, 2012 01:20 PM Due Date : Nov 8, 2012 01:20 PM

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **May 15, 2013 11:06 AM**

Resolution submitted by : (b)(3):6(f),(b)(4)

Edit

in (b)(3):6(f),(b)(4)

LIFELOCK-0132502

Request ID : 83219 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR (REDACTED) - Directory Traversal

By Jenner Holden on Dec 6, 2012 11:26 AM Due Date : Dec 7, 2012 04:26 PM

Status : Open
Priority : 2 - High

Request | Tasks (0) | Resolution | History

Description

Notes(4) Conversations Associate Change

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Network penetration test - Nov 13, 2012

Vulnerability Details (Links, CVE #'s etc):
Directory Traversal

Description & Remediation Info:
Directory Traversal flaw allows any file to be accessed from the operating system. This was leveraged by the penetration tester to acquire the SAM and SYSTEM files, which were used to acquire the local administrator password hash.

REDACTED

LIFELOCK-0132503

Determine if the flaw is the result of an application vulnerability with the Verisign web application, or the result of a configuration error on our part. Remediate accordingly.

Technician	Not Assigned	E-mail Id(s) To Notify	(b)(3):6(f),(b)(4)
Asset	-	Created By	Jenner Holden
Department	Products & Technology	SLA	High SLA
Template	IT Only - Vulnerability Remediation Request	Created Date	Dec 6, 2012 11:26 AM
DueBy Date	Dec 7, 2012 04:26 PM	Response DueBy Time	-
Last Update Time	Jul 2, 2013 10:43 AM		

Requester Details

Edit

Requester Name	Jenner Holden	E-mail Address	jenner.holden@lifelock.com
Contact number	(480) 457 - 2008	Mobile number	(b)(6),(b)(7)(C)
Department	Products & Technology	Date Vulnerability Announced	-
Laptop S/N	-	Location	-
Business Impact	-		

TOP

Discussion Notes

Add Notes

[4 note(s)]

User: (b)(3):6(f),(b)(4) **Private** Jul 1, 2013 03:51 PM

This server is still in use. I cannot update the application as its a built in web server. We could edit the server XML files to only listen on localhost but other than that I don't know what else to do for this.

Request ID : 83228

Edit | Assign ▼ | Actions ▼ | Reply ▼

VRR (Windows Domains) - Local Admin Password

By Jenner Holden on Dec 6, 2012 01:20 PM **Due Date** : Dec 11, 2012 01:20 PM

Status : Closed

Priority : 3 - Medium

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **Apr 4, 2013 09:42 AM**

Resolution submitted by : **Austin Appel**

Edit

Verified manually that the "Deny access from the network" GPO setting was successfully propagated. Will investigate using unique local administrator passwords in the future.

LIFELOCK-0132505

Request ID : 83232 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR (Multiple Linux) - Guessable Tomcat Manager Credentials

By Jenner Holden on Dec 6, 2012 01:55 PM Due Date : Dec 10, 2012 07:55 AM

Status : Open
Priority : 2 - High

Request | Tasks (0) | Resolution | History

Description

Notes(2) Conversations Associate Change

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Network Penetration Test, 11-12-12

Vulnerability Details (Links, CVE #'s etc):

Description & Remediation Info:
The Tomcat management console was identified to be using a default or guessable password.
An authenticated user can upload a custom WAR file (e.g. Java JSP command shell) and interact with the underlying operating system. This can result in a full compromise of the system or network as well as the disclosure of sensitive information and the denial-of- service to legitimate users.

The discovered credentials were manager/manager. Please change these credentials to meet our service account password requirements, and/or disable the tomcat manager web application, if it is not used.

Request Details

Edit

Status	Open	**Status**	-
Request Type	Service Request	**Category**	Information Security
Impact	Not Assigned	**Subcategory**	Vulnerability Remediation Requests
Urgency	Not Assigned	**Vulnerability Remediation Type**	Other
Priority	2 - High	**Vendor/Application/Protocol**	Not Assigned
Site	Not associated to any site	**Vendor Number**	-
Date of Request	Dec 6, 2012 01:52 PM	**CVE Reference**	CVE-
Date completed	-	**Remediation Status**	Closed - Remediated (to be verified)
Service Category	Not Assigned	**InfoSec Recommended Course of Action**	Apply Fix - Defined SLA
Group	Information Security	**Action Decision**	Not Assigned
Technician	Austin Appel	**E-mail Id(s) To Notify**	(b)(3):6(f),(b)(4)
Asset	-	**Created By**	Jenner Holden
Department	Products & Technology	**SLA**	High SLA
Template	IT Only - Vulnerability Remediation Request	**Created Date**	Dec 6, 2012 01:55 PM
DueBy Date	Dec 10, 2012 07:55 AM	**Response DueBy Time**	-
Last Update Time	Jun 6, 2013 08:28 PM		

Requester Details

Edit

Requester Name	Jenner Holden	E-mail Address	jenner.holden@lifelock.com
Contact number	(480) 457 - 2008	Mobile number	(b)(6),(b)(7)(C)
Department	Products & Technology	Date Vulnerability Announced	-
Laptop S/N	-	Location	-
Business Impact	-		

TOP

Discussion Notes

Add Notes

[2 note(s)]

User: (b)(3):6(f),(b)(4) **Private** Apr 2, 2013 09:31 AM

This has been resolved.

User: (b)(3):6(f),(b)(4) **Private** Mar 27, 2013 12:36 PM

Updated the tomcat users.xml file, and removed the default credentials. We're just waiting on tomcat reboots now to make them get applied.

Request ID : 83627 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR - [redacted] - Web VPN - No Longer Needed?

By Jenner Holden on Dec 17, 2012 02:38 PM Due Date : Dec 21, 2012 02:38 PM

Status : Open
Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **Mar 15, 2013 12:59 PM**

Resolution submitted by : **David Henry**

Edit

This device is not in use. It will be turned off and taken off line.

LIFELOCK-0132509

Request ID : 83629 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR - Check_MK - No Authentication

By Jenner Holden on Dec 17, 2012 02:52 PM **Due Date** : Dec 20, 2012 02:52 PM

Request | Tasks (0) | Resolution | History

Description Notes(1) Conversations A

Machine Name and/or IP:
All Check_MK Agents

Discovery Method & Date:
Penetration Test - November 2012

Vulnerability Details (Links, CVE #'s etc):

Description & Remediation Info:
The Check_MK agent appears to dump system information to any TCP connection...there does not appear to be any authentication. Can Check_MK be configured so only authorized this information?

For example:
REDACTED
<<<check_mk>>>
Version: 1.1.10p3
AgentOS: linux

Group	Information Security	Action Decision	Not Assigned
Technician	Austin Appel	Asset	-
Created By	Jenner Holden	Department	Products & Technology
SLA	Medium SLA	Template	IT Only - Vulnerability Remediation Requ
Created Date	Dec 17, 2012 02:52 PM	DueBy Date	Dec 20, 2012 02:52 PM
Response DueBy Time	-	Last Update Time	Jun 6, 2013 08:28 PM

Requester Details

Edit

Requester Name	Jenner Holden	E-mail Address	jenner.holden@lifelock.com
Contact number	(480) 457 - 2008	Mobile number	(b)(6),(b)(7)(C)
Department	Products & Technology	Date Vulnerability Announced	-
Laptop S/N	-	Location	-
Business Impact	-		

Discussion Notes

Add Notes

User: (b)(3):6(f),(b)(4)

Private

This was updated back in January. Please re-scan.

# configure the IP address(es) of your Nagios server here:
only_from = REDACTED

Request ID : 83631

Edit | Assign ▼ | Actions ▼ | Reply ▼

VRR REDACTED - SVN Information Disclosure

By Jenner Holden on Dec 17, 2012 02:59 PM Due Date : Dec 21, 2012 02:59 PM

Status : Closed

Priority : 4 - Low

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : **Dec 20, 2012 09:25 AM**

Resolution submitted by : **Jenner Holden**

Edit

Confirmed - the issue has been resolved.

REDACTED

oracle@REDAC

```
HOUDANE @prem>select USERNAME,LOCK_DATE,ACCOUNT_STATUS,EXPIRY_DATE,DEFAULT_TABLESPACE,PROFILE from dba_users where USERNAME in ('APPQOSSYS','CTXSYS','DIP','
EXFSYS','MDDATA','MDSYS','OLAPSYS','ORACLE_OCM','ORDDATA','ORDPLUGINS','ORDSYS','OUTLN','OWBSYS','SCOTT','SI_INFORMTN_SCHEMA','SPATIAL_CSW_ADMIN_USR','SPATIA
L_WFS_ADMIN_USR','TSMSYS','WMSYS','XDB') order by 1 asc;

USERNAME                       LOCK_DATE          ACCOUNT_STATUS                 EXPIRY_DATE        DEFAULT_TABLESPACE             PROFILE
------------------------------ ------------------ ------------------------------ ------------------ ------------------------------ ----------
APPQOSSYS                      05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
CTXSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
DIP                            05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
EXFSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
MDDATA                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
MDSYS                          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
OLAPSYS                        05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
ORACLE_OCM                     05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
ORDDATA                        05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
ORDPLUGINS                     05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
ORDSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
OUTLN                          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSTEM                         DEFAULT
OWBSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
SCOTT                          19-MAY-11          EXPIRED & LOCKED               19-MAY-11          USERS                          DEFAULT
SI_INFORMTN_SCHEMA             05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
SPATIAL_CSW_ADMIN_USR          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
SPATIAL_WFS_ADMIN_USR          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
TSMSYS                         30-JUL-11          EXPIRED & LOCKED               30-JUL-11          USERS                          DEFAULT
WMSYS                          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
XDB                            05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT

20 rows selected.

HOUDANE @prem>/date
Thu Mar 14 10:37:45 MST 2013
```

[redacted]

oracle@RE

```
SYS AS SYSDBA@p11dw>select USERNAME,LOCK_DATE,ACCOUNT_STATUS,EXPIRY_DATE,DEFAULT_TABLESPACE,PROFILE from dba_users where USERNAME in ('APPQOSSYS','CTXSYS','D
IP','EXFSYS','MDDATA','MDSYS','OLAPSYS','ORACLE_OCM','ORDDATA','ORDPLUGINS','ORDSYS','OUTLN','OWBSYS','SCOTT','SI_INFORMTN_SCHEMA','SPATIAL_CSW_ADMIN_USR','S
PATIAL_WFS_ADMIN_USR','TSMSYS','WMSYS','XDB') order by 1 asc;

USERNAME                       LOCK_DATE          ACCOUNT_STATUS                 EXPIRY_DATE        DEFAULT_TABLESPACE             PROFILE
------------------------------ ------------------ ------------------------------ ------------------ ------------------------------ ----------
APPQOSSYS                      05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
CTXSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
DIP                            05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
EXFSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
MDDATA                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
MDSYS                          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
OLAPSYS                        05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
ORACLE_OCM                     05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
ORDDATA                        05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
ORDPLUGINS                     05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
ORDSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
OUTLN                          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSTEM                         DEFAULT
OWBSYS                         05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
SCOTT                          27-APR-11          EXPIRED & LOCKED               27-APR-11          USERS                          DEFAULT
SI_INFORMTN_SCHEMA             05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
SPATIAL_CSW_ADMIN_USR          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
SPATIAL_WFS_ADMIN_USR          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          USERS                          DEFAULT
WMSYS                          05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
XDB                            05-SEP-10          EXPIRED & LOCKED               05-SEP-10          SYSAUX                         DEFAULT
```

REDACTED

oracle REDA

```
SYS AS SYSDBA@pinforep>select USERNAME,LOCK_DATE,ACCOUNT_STATUS,EXPIRY_DATE,DEFAULT_TABLESPACE,PROFILE from dba_users where USERNAME in ('APPQOSSYS','CTXSYS','
DIP','EXFSYS','MDDATA','MDSYS','OLAPSYS','ORACLE_OCM','ORDDATA','ORDPLUGINS','ORDSYS','OUTLN','OWBSYS','SCOTT','SI_INFORMTN_SCHEMA','SPATIAL_CSW_ADMIN_USR','
SPATIAL_WFS_ADMIN_USR','TSMSYS','WMSYS','XDB') order by 1 asc;

USERNAME                       LOCK_DATE         ACCOUNT_STATUS                 EXPIRY_DATE       DEFAULT_TABLESPACE             PROFILE
------------------------------ ----------------- ------------------------------ ----------------- ------------------------------ ---------------
APPQOSSYS                      05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
CTXSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
DIP                            05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
EXFSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
MDDATA                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
MDSYS                          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
OLAPSYS                        05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
ORACLE_OCM                     05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
ORDDATA                        05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
ORDPLUGINS                     05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
ORDSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
OUTLN                          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSTEM                         DEFAULT
OWBSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
SCOTT                          27-APR-11         EXPIRED & LOCKED               27-APR-11         USERS                          DEFAULT
SI_INFORMTN_SCHEMA             05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
SPATIAL_CSW_ADMIN_USR          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
SPATIAL_WFS_ADMIN_USR          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
WMSYS                          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
XDB                            05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
```

[redacted]

oracle RED

```
SYS AS SYSDBA@pinforep>/

USERNAME                       LOCK_DATE         ACCOUNT_STATUS                 EXPIRY_DATE       DEFAULT_TABLESPACE             PROFILE
------------------------------ ----------------- ------------------------------ ----------------- ------------------------------ ---------------
APPQOSSYS                      05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
CTXSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
DIP                            05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
EXFSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
MDDATA                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
MDSYS                          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
OLAPSYS                        05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
ORACLE_OCM                     05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
ORDDATA                        05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
ORDPLUGINS                     05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
ORDSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
OUTLN                          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSTEM                         DEFAULT
OWBSYS                         05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
SCOTT                          27-APR-11         EXPIRED & LOCKED               27-APR-11         USERS                          DEFAULT
SI_INFORMTN_SCHEMA             05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
SPATIAL_CSW_ADMIN_USR          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
SPATIAL_WFS_ADMIN_USR          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         USERS                          DEFAULT
WMSYS                          05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT
XDB                            05-SEP-10         EXPIRED & LOCKED               05-SEP-10         SYSAUX                         DEFAULT

19 rows selected.

SYS AS SYSDBA@pinforep>!date
Thu Mar 14 10:41:44 MST 2013
```

Back to previous view

[EN-374] Vulnerability Remediation - Hidden Directory Enumeration

Created: 19/Nov/12 Updated: 07/Aug/14 Resolved: 30/Jun/14

Status:	Closed
Project:	Webstore Acquisition II
Component/s:	None
Affects Version/s:	None
Fix Version/s:	None

Type:	Story	**Priority:**	Critical
Reporter:	Jenner Holden	**Assignee:**	(b)(3) 6f(b)(4)
Resolution:	Complete	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Description

SR# 81926 (Medium)

This vulnerability was discovered during a recent penetration test.

The web application exposes the presence of a directory in the site. Although the directory does not list its content, the information may help an attacker to develop further attacks against the site. For example, by knowing the directory name, an attacker can guess its content type and possibly file names that reside in it or sub-directories under it. The more sensitive the content is, the more severe the issue is.

Typically, a hidden directory can be detected when a "403 - Forbidden" response is issued by the web server, but any response that is not "404 - Not Found" can be used to detect the presence of a directory. For example, some web servers issue "courtesy redirects" when the trailing slash of a directory is omitted.
The following hidden directories were detected:
/cgi-bin/
/common/
/scripts/
/images/

If the forbidden resource is not required, remove it from the site. If possible, issue a "404 - Not Found" response status code instead of a "403 - Forbidden" or other responses. This change will obfuscate the presence of the directory in the site and will prevent the site structure from being exposed.

It's unclear which site the tester is referring to with this finding, please check www.lifelock.com, secure.lifelock.com, and lifelock.jobs.

Comments

Comment by James Moler [27/Jun/14]

(b)(3) 6f(b)(4) This legacy story applies to WWW only. The hidden directories don't exist on Webstore/Member Portal.

Comment by (b)(3) 6f(b)(4) [30/Jun/14]

Confirmed that these findings are no longer relevant to the current instance of the website. Issue can be closed.

(b)(3) 6f(b)(4)
Sr. Application Security Engineer | LifeLock® - Relentlessly Protecting Your Identity™
(b)(3) 6f(b)(4)

LIFELOCK-0132514

Generated at Fri Sep 05 15:46:35 MST 2014 by Austin Appel using (b)(3) 6f(b)(4)

Request ID : 82261 | Edit | Close | Assign | Actions | Reply

VRR - [redacted] Default Credentials

By Jenner Holden on Nov 12, 2012 02:00 PM Due Date : Nov 14, 2012 08:00 AM

Status : Open
Priority : 2 - High

Request | Tasks (0) | Resolution | History

Description

Attachments (1) | Conversations | New Problem | Associate Change

Machine Name and/or IP:
[redacted]

Discovery Method & Date:
[redacted]

Vulnerability Details (Links, CVE #'s etc):
Oracle Default Credentials

Description & Remediation Info:
Please review the following list of user accounts, and validate that none of them are using default credentials. Please remove/disable any accounts that are not needed. Also, remove the remote login file for any system accounts that do not require remote login capabilities.

```
APPQOSSYS
CTXSYS
DIP
EXFSYS
MDDATA
MDSYS
OLAPSYS
ORACLE_OCM
ORDDATA
ORDPLUGINS
ORDSYS
OUTLN
OWBSYS
SCOTT
SI_INFORMTN_SCHEMA
SPATIAL_CSW_ADMIN_USR
SPATIAL_WFS_ADMIN_USR
TSMSYS

WMSYS
XDB
```

Attachments : Ticket request 82261.docx (308.81 KB)

TOP

Reply | Forward

TOP

Requester Conversations | [View All Conversations]

- System on Nov 12, 2012 02:00 PM
- System on Mar 14, 2013 10:51 AM
- System on Jun 6, 2013 08:28 PM
- System on Jul 19, 2013 09:40 AM
- System on Jul 19, 2013 09:41 AM
- System on Jul 19, 2013 09:41 AM

Request Details | Edit

Status	Open	Request Type	Service Request
Category	Information Security	Impact	Not Assigned
Subcategory	Vulnerability Remediation Requests	Urgency	Not Assigned
Vulnerability Remediation Type	Other	Priority	2 - High
Vendor/Application/Protocol	Oracle	Site	Not associated to any site
Vendor Number	-	Date of Request	Nov 12, 2012 01:56 PM
CVE Reference	CVE-	Date completed	-
Remediation Status	Closed - Remediated (to be verified)	Service Category	Not Assigned
InfoSec Recommended Course of Action	Apply Fix - Defined SLA	Group	Information Security
Action Decision	Not Assigned	Technician	Austin Appel
Asset	-	Created By	Jenner Holden
Department	Products & Technology	SLA	High SLA
Template	IT Only - Vulnerability Remediation Request	Created Date	Nov 12, 2012 02:00 PM
DueBy Date	Nov 14, 2012 08:00 AM	Response DueBy Time	-
Last Update Time	Jul 19, 2013 09:41 AM		

Requester Details | Edit

Requester Name	Jenner Holden	E-mail Address	jenner.holden@lifelock.com
Contact number	(480) 457 - 2008	Mobile number	[redacted]
Department	Products & Technology	Date Vulnerability Announced	-
Laptop S/N	-	Location	-
Business Impact	-		

Request ID : 82261 Edit Close Assign ▼ Actions ▼ Reply ▼

VRR - [redacted] - Default Credentials

By Jenner Holden on Nov 12, 2012 02:00 PM Due Date : Nov 14, 2012 08:00 AM

Status : Open
Priority : 2 - High

Request | Tasks (0) | Resolution | History

Search Solutions

Submitted on : Mar 14, 2013 10:51 AM

Resolution submitted by : (b)(3)-6(f),(b)(4)

Edit

Aside of SCOTT (this account will be removed from all current database environments and future database environments as part of the build process), the other accounts are used within various components of the Oracle product line. They are used indirectly by the Oracle Software thus they are Expired and Locked and not accessed directly. The accounts are necessary and thus will not be removed.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 19
TO EXPERT REPORT OF DR. ERIC B. COLE

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 20
TO EXPERT REPORT OF DR. ERIC B. COLE

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 21
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 22
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 23
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: Jenner Holden [/O=LIFELOCK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=JENNER.HOLDEN]
Sent: Thursday, December 06, 2012 10:27 AM
To: (b)(3):6(f),(b)(4)
Subject: FW: Your request, <<VRR [redacted] - Directory Traversal>> has been logged with request id ##83219##

Importance: High

FYI – I submitted a VRR for the directory traversal issue we discussed.

Jenner Holden
Director of Information Security | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2008 Office | (b)(6),(b)(7)(C) Cell
Jenner.Holden@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: (b)(3):6(f),(b)(4)
Date: Thursday, December 6, 2012 11:26 AM
To: Jenner Holden <jenner.holden@lifelock.com>
Subject: Your request, <<VRR [redacted] - Directory Traversal>> has been logged with request id ##83219##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 83219. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 83219
Priority : High
Urgency :
Status : Open

Due By: Dec 26, 2012 11:26 AM
Subject : VRR [redacted] - Directory Traversal.
Description : **Machine Name and/or IP:**
[redacted]

Discovery Method & Date:
Network penetration test - Nov 13, 2012

Vulnerability Details (Links, CVE #'s etc):
Directory Traversal

Description & Remediation Info:
Directory Traversal flaw allows any file to be accessed from the operating system. This was leveraged by the penetration tester to acquire the SAM and SYSTEM files, which were used to acquire the local administrator password hash.

http://R [redacted] ..\..\..\..\..\..\..\windows\repair\sam
REDACTED [redacted] ..\..\..\..\..\..\..\windows\repair\system

Determine if the flaw is the result of an application vulnerability with the (b)(3):6 (f),(b)(4) web application, or the result of a configuration error on our part. Remediate accordingly.

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 24
TO EXPERT REPORT OF DR. ERIC B. COLE

From: (b)(3):6(f),(b)(4)

Sent: Thursday, December 06, 2012 12:20 PM
To: Jenner Holden
Subject: Your request, <<VRR (Windows Domains) - Local Admin Password>> has been logged with request id ##83228##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 83228. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 83228
Priority : Medium
Urgency :
Status : Open

Due By: Jan 15, 2013 01:20 PM
Subject : VRR (Windows Domains) - Local Admin Password.
Description : **Machine Name and/or IP:**
Windows Domains

Discovery Method & Date:
Network Pen-Test, 11-12-12

Vulnerability Details (Links, CVE #'s etc):

Description & Remediation Info:
The local administrator credentials were verified as being reused throughout the enterprise.
The reuse of passwords reduces the need for an attacker to compromise multiple systems in order to increase network visibility. Specifically, an attacker simply needs to enumerate one successful exploit and they have inherently exploited all affected systems.

The penetration tester leveraged this issue to access all Windows PCI servers.

Please evaluate potential solutions, including:

1 - Using unique local administrator passwords for each server
2 - Enabling the "Deny access from the network" GPO setting to the local administrator. Effectively blocking the local administrator account from authenticating over the network.

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:

Close Request

Thank you for contacting LifeLock(R) Helpdesk.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 25
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: (b)(3):6(f),(b)(4)
Sent: Thursday, December 06, 2012 12:55 PM
To: Jenner Holden
Subject: Your request, <<VRR (Multiple Linux) - Guessable Tomcat Manager Credentials>> has been logged with request id ##83232##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 83232. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 83232
Priority : High
Urgency :
Status : Open

Due By: Dec 26, 2012 01:55 PM
Subject : VRR (Multiple Linux) - Guessable Tomcat Manager Credentials.
Description : **Machine Name and/or IP:**
REDACTED

Discovery Method & Date:
Network Penetration Test, 11-12-12

Vulnerability Details (Links, CVE #'s etc):

Description & Remediation Info:
The Tomcat management console was identified to be using a default or guessable password.
An authenticated user can upload a custom WAR file (e.g. Java JSP command shell) and interact with the underlying operating system. This can result in a full compromise of the system or network as well as the disclosure of sensitive information and the denial-of- service to legitimate users.

The discovered credentials were manager/manager. Please change these credentials to meet our service account password requirements...and/or disable the tomcat manager web application, if it is not used.

Please evaluate all tomcat installs for this same issue.

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 26
TO EXPERT REPORT OF DR. ERIC B. COLE

***This Attachment contains redactions which are identified in the document by blacked out text or the text "REDACTED."**