OIG EVALUATION

Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices

Report No. ER 16-03 // September 2016

Submitted by
TACG, LLC
Contract Number: 29FTC116C0050

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

Office of Inspector General

September 30, 2016

MEMORANDUM

TO: Chairwoman Edith Ramirez
Commissioner Maureen K. Ohlhausen
Commissioner Terrell McSweeny

FROM: Roslyn A. Mazer
Inspector General

SUBJECT: Transmittal of the Final Report, *Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices*

Attached is the Office of Inspector General Report ER 16-03, *Opportunities Exist to Accelerate Maturation of the FTC's Information Technology Governance Practices*. The evaluation was performed by TACG LLC, in accordance with the Quality Standards for Inspection and Evaluation promulgated by the Council of Inspectors General on Integrity and Efficiency.

Our findings include two types of IT Governance Program weaknesses: first, findings that affect all investments that are subject to the FTC Governance Process to varying degrees, and second, weaknesses that are project-specific to the electronic discovery (eDSS) and mobile device project that we studied in the evaluation. The OIG's identification of these weaknesses showed that while the Governance Program is improving, there remain significant opportunities to accelerate maturation of the Program. The report makes 15 recommendations: 6 pertaining to the Governance Program, and 9 that are specific to individual projects (5 for the eDSS project, 3 for the mobile device project, and 1 pertaining to Controlled Unclassified Information).

Management provided written comments dated September 30, 2016, which are reproduced in Appendix D. Management concurred in all 15 recommendations and provided action plans to address each of the recommendations, with scheduled completion dates between Q1 2017 through Q2 2018. The OIG's analysis of management's response, dated September 30, 2016, is reproduced in Appendix E. We will examine the effectiveness of the planned improvements to the FTC's Information Technology Governance Practices as part of the Fiscal Year 2017 Federal Information Security Modernization Act (FISMA) evaluation. We also will continue to monitor

management progress in implementing open recommendations from previous FISMA and other OIG reporting.

We appreciate the cooperation from management and staff and acknowledge the commitment to improving information security and privacy at the FTC. If you have any questions, please do not hesitate to contact me.

Cc: Heather Hippsley, Chief of Staff
David Robbins, Executive Director
David C. Shonka, Acting General Counsel
Patricia Bak, Deputy Executive Director
Monique Fortenberry, Deputy Executive Director
Raghav Vajjhala, Chief Information Officer
Jeffrey Smith, Assistant Director Information Assurance
Katherine Race Brin, Chief Privacy Officer
Alexander C. Tang, Senior Attorney, Office of General Counsel
Jeffrey D. Nakrin, Director Records & Filing Office
David Rebich, Chief Financial Officer and Performance Improvement Officer
Valerie Green, Deputy Performance Improvement Officer

Executive Summary

The Federal Trade Commission (FTC) is an independent law enforcement agency founded in 1914 with the passage of the Federal Trade Commission Act. The mission of the FTC is to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing consumer choice and public understanding of the competitive process, and accomplishing this without unduly burdening legitimate business activity. To execute its broad mandate, the FTC employs a variety of tools, including law enforcement, rulemaking, advocacy, research and studies on marketplace trends, and consumer and business outreach and education.

The Importance of Information Technology Governance

FTC depends on information technology (IT) to complete its missions and associated business objectives. In accordance with federal law, (e.g., the Federal Information Security Modernization Act of 2014 (FISMA), Public Law No: 113-283) and Office of Management and Budget (OMB) policy (e.g., OMB Circular A-130, *Managing Information as a Strategic Resource*) the Chief Information Officer (CIO), in coordination with FTC Bureaus and Offices and appropriate governance boards, defines processes and policies to address information resources appropriately. This includes establishing policies and procedures that ensure needed information resources are appropriately planned, acquired, operated and maintained, and deliver needed support securely and efficiently.

IT governance is the framework an organization is to use to align its IT strategy with its business strategy and ensure that the organization meets its mission and associated strategic goals and objectives. OMB consolidated its various policies and guidance affecting IT governance in its revision of OMB Circular A-130 in July 2016. OMB Circular A-130 identifies a number of objectives for a federal governance structure including —

- Using open data standards to the maximum extent possible when implementing IT systems;
- Maintaining appropriate measurements to evaluate the cost, schedule, and overall performance variances of IT projects across the portfolio leveraging processes such as IT investment management, enterprise architecture, and other agency IT or performance management processes;
- Maintaining agency-wide data governance policies that clearly establish the roles, responsibilities, and processes by which agency personnel manage information and the relationships among technology, data, agency programs, strategies, legal and regulatory requirements, and business objectives;
- Phasing out as rapidly as possible, unsupported systems and planning and budgeting activities for all IT systems and services and incorporating migration planning and resourcing to accomplish this requirement;

- Designating the CIO as a member of governance boards that inform decisions regarding IT resources to provide for early matching of appropriate information resources with program objectives. The CIO may designate, in consultation with other senior agency officials, other agency officials to act as their representative to fulfill aspects of this responsibility so long as the CIO retains accountability;

- Fully integrating information security and privacy into the system development process;

- Maintaining processes for the CIO to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective;

- Ensuring security, privacy, accessibility, records management, and other relevant requirements are included in solicitations; and

- Ensuring acquisition strategies, plans, and requirements (as described in FAR Part 7), or interagency agreements (such as those used to support purchases through another agency) that include IT, are reviewed and approved by the purchasing CIO.

The FTC initiated its IT Governance Program with issuance of its IT Governance Program Charter in November of 2011 in compliance with OMB policy then in place. The FTC updated its IT Governance Program Charter in August 2014. Under the FTC organizational structure, the IT Governance Board (ITGB) serves as the top-level component of the FTC's overall IT governance structure. The FTC Executive Director (ED) serves as the ITGB Chair and reports to the FTC Chairwoman. The FTC CIO reports to the ED and serves as the Chair of the IT Council, as a Co-Chair of the IT Business Council, and as member of the ITGB.[1]

The FTC Officer of Inspector General (OIG) included evaluation of the FTC IT Governance Program in its FISMA evaluations commencing in FY 2011. Each year, the OIG determined that the IT Governance Program was maturing, but the improvement rate was slow; the governance workflow was not documented in Standard Operating Procedures or Work Instructions; and the Program retained a project focus instead of the enterprise-wide focus intended in OMB and National Institute of Standards and Technology (NIST) guidance (e.g., Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*).

Scope and Objectives

As a follow onto its FY 2015 FISMA evaluation, the OIG tasked TACG, LLC, to perform an evaluation of the governance practices the FTC uses to plan, evaluate, fund, and monitor IT projects. The objective was to determine if the FTC governance process includes procedures and controls to identify and resolve potential problems and minimize the risk of project failure. The evaluation included review of the FTC Governance Program Charter and associated FTC procedural documents, project documents generated as part of the Governance Process, and

[1] Under the 2014 IT Governance Program Charter, the CIO was a non-voting member of the ITGB and the ITBC. The CIO role in the ITGB and the ITBC was changed in FY 2016 to a voting membership.

Meeting Minutes and other artifacts documenting Governance Board activities and decisions. Work on this evaluation commenced on July 24, 2015 with data collection completed on March 30, 2016. As part of this effort, TACG, with OIG review and concurrence, identified three projects (two approved for FTC funding and a government-wide program that might be reflected in an FTC project) for inclusion in the analysis: the e-Discovery Support System (eDSS), the Mobile Device Project, and FTC planning for information system changes resulting from the government-wide Controlled Unclassified Information (CUI) program. The three projects each has a high impact on the FTC mission and the day-to-day activities of its work force and contractors.

- e-Discovery Support System (eDSS) – The eDSS project was initiated in 2013 to replace and modernize tools used by the FTC to collect and analyze information produced as part of FTC litigation activities. The new eDSS was planned to be more reliable, have expanded capabilities, and be capable of processing the large volumes of data associated with FTC litigation activities in shorter timeframes than legacy software. The eDSS is principally to support the Bureau of Competition (BC) and the Bureau of Consumer Protection (BCP), but may be used by the Bureau of Economics and Offices with large-scale data collection and analysis needs.

- Mobile Device Project – The Mobile Device Project is part of the FTC initiative to modernize the mobile computing and communications devices used by FTC personnel. The Mobile Device Project evaluated was the replacement and upgrade of the FTC's Blackberry personal data assistant (telephone and e-mail) with state-of-the-art smart phones.

- Controlled Unclassified Information (CUI) – The National Archives and Records Administration (NARA) is the Executive Agent for a program to standardize the categorization, marking, and safeguarding of information that is sensitive, but unclassified. FTC information systems may need to be modified to address changes in marking and labeling requirements originating from NARA and CUI protection requirements originating from the National Institute of Standards and Technology (NIST). Current direction from NARA is to pause changes involving categorization, labeling, and marking. Current direction from NIST is to implement moderate level safeguarding measures to all information and systems that collect, transmit, process, or store CUI. The OIG evaluated the process for integrating current direction and potential CUI changes into the governance process.

Under FTC governance policy, these projects are subject to review and approval by the Governance Boards.

Results of the Evaluation

The FTC IT Governance Program Charter is based on OMB Circular A-130, *Management of Federal Information Resources,* Nov 28, 2000, and the Federal CIO's "25 Point Implementation Plan to Reform Federal Information Technology Management" (December 2010). The Program Charter, states as follow for the Scope and Governance Principles of the Program:

> To increase transparency and proactively manage risk, all IT investments are within the scope of IT governance, regardless of the estimated cost and the organization managing the investments. This includes the acquisition, development, upgrade or maintenance of all hardware, software, applications, systems, and related services investments supporting FTC business lines and management processes. While the scope of IT governance covers all types of IT investments, the level of oversight depends on type of investment and should be commensurate with its complexity and risk.

The Governance Program Charter identifies the primary decision support artifact as a Business Case Analysis (BCA). A Business Case Analysis is a structured methodology and document that aids decision making by identifying and comparing alternatives and by examining the mission and business impacts (both financial and non-financial), risks, and sensitivities. The FTC Governance Program Charter defines two Business Case Analysis formats: an Executive Summary required for all projects, and a Full Business Case Analysis. The Executive Summary provides a high-level view of the project and "explains the project and its goals in concise and plain language." The full Business Case Analysis "expands on the executive summary and provides additional details." The focus of an FTC Business Case Analysis in the Governance Program is the decision to approve an individual project. Once an approval decision is received, the Business Case Analysis becomes an historical artifact.

FTC IT investments generally include acquisition of goods or services and are therefore subject to the Federal Acquisition Regulation (FAR), Parts 7 and 39. The principal artifact under FAR Part 7 is the Acquisition Plan which

- identifies those milestones at which decisions should be made (see paragraph (b) (18) of this section); and

- addresses all the technical, business, management, and other significant considerations that will control the acquisition.

Guidance for Acquisition Plan preparation includes the elements of a Business Case Analysis and consideration for selection of the appropriate acquisition approach, controlling the acquisition process and performance after award, and a requirement for a discussion of risk and risk management approaches that provides for inclusion of schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, funding availability, and program management risk. The Acquisition Plan is also a "living document," requiring revision as the acquisition moves from inception to conclusion. FAR acquisition planning requirements were tailored for the FTC in the *OCIO Acquisition Strategy for Information Technology*.

Both the eDSS and mobile device projects met the FTC criteria for a large, complex, high performance risk investment and require a full Business Case Analysis and an Acquisition Plan. However, neither project had an Acquisition Plan. And, critically, neither the Governance Program charter nor the IT Acquisition Strategy described how the Governance Program would work in concert with the Acquisition Strategy to maximize the potential for successful outcomes

(i.e., goods and services that meet FTC needs for functionality, reliability, security, and cost effectiveness).

Two types of governance weaknesses were identified in the evaluation: first are those findings summarized below related to the Governance Process. These findings affect all investments subject to the FTC Governance Program to varying degrees. For example, weaknesses affecting replacement of Blackberrys with smart phones will have a low performance risk because the smart phones are commodity items with known performance characteristics, and limited modification is required. The eDSS project has a high performance risk and associated cost impact because specific functional requirements must be identified as well as criteria for determining successful implementation and ongoing performance under varying workloads.

The second type of weaknesses identified are project specific. These weaknesses relate to a failure to follow FTC procedures and are reflected in the recommendations listed below and are described in the body of the report.

The following are the OIG's key assessments of how Governance Process weaknesses affected the two ongoing acquisitions for eDSS and mobile devices and how these same weaknesses could, if unaddressed, complicate and delay the FTC's ability to assimilate current guidance and coming requirements for the CUI program as well as future IT acquisitions to which the FTC Governance Program applies:

1. **Policy conflicts between the FTC IT Governance Program Charter and the FAR / *FTC OCIO Acquisition Strategy for Information Technology* increase the potential for inconsistent planning and oversight and delivery of products and services that do not meet FTC requirements.** The FTC governance practices are defined by the FTC IT Governance Program Charter. The Charter identifies the Business Case Analysis as the primary decision support artifact supporting the governance process. There is limited guidance provided that describes the contents of a Business Case Analysis. The content requirements are stated in broad terms in the Business Case Analysis templates. For example, the template for a Full Business Case Analysis requires the submitter to "describe sources of cost and non-cost data for the alternatives, level of confidence in the data and any recommendations to address insufficiency of data or low level of confidence."

The FTC's Governance Program Charter identifies the Business Case Analysis as the primary decision document, but fails to mention that FTC acquisitions are also governed by the Federal Acquisition Regulation (FAR) Part 7. The FAR establishes specific requirements for identifying and justifying goods or services from the initial conception of an acquisition to disposition of goods and services when no longer required. FAR Part 7 requirements are included in the *FTC OCIO Acquisition Strategy for Information Technology,* September 2011, which states that proponents of all agency IT-related expenditures are to detail the Acquisition Plan elements referenced in FAR 7.1 05 *et seq*.

The principal document for addressing FAR acquisition requirements is the Acquisition Plan. The scope of an Acquisition Plan is broader than the scope of a Business Case Analysis; thus, the

acquisition elements of a Business Case Analysis have a corresponding element in an Acquisition Plan, but elements of a Business Case Analysis do not include all Acquisition Plan elements. This results in a situation where a BCA can be prepared in accordance with FTC guidance and still be non-compliant with the FAR. In response to the OIG request, The OCIO did not provide FAR-compliant Acquisition Plans for either the eDSS or the mobile device project.

Lack of FAR compliance had a significant impact on the eDSS project. The Business Case Analysis supports a decision regarding project funding. The Acquisition Plan provides a structure for controlling and managing an acquisition from inception to contract completion. Had the eDSS followed FAR procedures, the cost and workload estimate deficiencies identified in the Business Case Analysis and the deferred performance and evaluation procedures (e.g., performance criteria and solicitation documents) would have been reflected as milestones or stage gates where deficiencies were resolved before the project proceeded.

The mobile device project would also have benefitted from an Acquisition Plan. While the Acquisition Plan would be abbreviated, it would have helped ensure completion of planned test reports and project completion in accordance with the project schedule. While use of FAR analysis and acquisition management practices do not guarantee project success, they minimize performance risk and allow for timely problem resolution.

2. **Governance decisions did not include milestones or other restrictions to monitor and verify resolution of identified deficiencies.** The Governance Board approved project funding when significant Business Case Analysis elements were identified as deficient or omitted. This allowed deficiencies to remain unresolved and adversely impact project performance and oversight. For example, even though eDSS cost data was identified as incomplete and inaccurate, and omitted artifacts such as performance metrics were deferred, no milestones or "stage gates" were established that would provide for subsequent Governance Board review and approval to verify that identified deficiencies were resolved before the project was authorized to proceed. For example, eDSS analyses did not include performance of a workload assessment where testing is performed to determine the relationship between the current data structures and search approaches against the structures and approaches used by bidders for the eDSS contract. This testing would validate the reasonableness of workload projections, providing the FTC with a better understanding of how the system will perform in a production environment. An improved understanding of performance under production conditions could have helped the FTC avoid hosting the eDSS on an undersized configuration with poor/slow performance and reliability. eDSS performance is so poor that FTC users are seeking alternatives.

3. **BCAs provided to the Governance Boards did not include an appropriate workload analyses.** A workload analysis is intended to support three acquisition objectives: analysis of price models that are workload sensitive (e.g., Software as a Service (SaaS)); estimate the computing and network resources needed to support the anticipated workload (e.g., impact of differences in search and data storage strategies on requirements and performance); and evaluate the impact of workload changes (e.g.,

growth, spikes, and cyclical fluctuations) on performance and pricing. The eDSS did not include a workload analysis. Products were evaluated as part of the eDSS solicitation, but this analysis and associated demonstrations and testing focused on functionality and not workload estimation. The workload analysis is a key decision factor when IT solutions are intended for installation on the FTC infrastructure. The workload analysis is compared against existing workload capabilities and projected growth to support an OCIO/Governance Board decision to install a particular solution on the infrastructure or on an outside service.

The FTC did develop an eDSS workload analysis. The workload projection substantially underestimated resource requirements. After award and installation of the eDSS software on the FTC infrastructure, FTC determined that the workload analysis substantially under estimated resource requirements. The underestimate was due to different storage approaches and different resource utilization rates of the new eDSS software versus the legacy software.

4. **FTC Governance Board procedures do not include a formal escalation process.** Projects may be expected to encounter problems during execution. The Governance Board does not have procedures in place to identify project problems and escalate those problems to a management level that ensures timely resolution. This has resulted in problem projects continuing for multiple years without resolution. For example, the eDSS acquisition did not include the Legal features such as Litigation Hold necessary to support FTC e-discovery needs and the processing capacity to effectively support FTC workloads. These deficiencies required Bureaus to use manual procedures or other products to compensate for functional deficiencies and to take turns preparing productions to opposing counsel or court to compensate for the lack of processing capability. These deficiencies were identified early in the eDSS contract performance period and resulted in a number of efforts, largely ineffective, to resolve the problems.

Recommendations

To address the findings in this evaluation, we identified the following 15 recommendations for improvement, 6 that are directly related to the Governance Program, and 9 that are specific to individual projects (5 for the eDSS project, 3 for the mobile device project, and 1 for the CUI project). The focus of the first set of recommendations is to suggest improvements in the Governance Program to increase the potential for successful future acquisitions. Project-specific recommendations are intended to identify problem areas and limit continued spending where there is high risk of project failure. For example, the eDSS project should be terminated, with further spending limited to support of ongoing projects. The focus of the eDSS effort should be a new acquisition, using the lessons learned on the past acquisition. The recommendation for the CUI evaluation focuses on ensuring that FTC is in position to implement changes as required to support the CUI program as guidance is released:

1. Complete applicable Business Case Analysis elements, including a description of security requirements and how they will be met, functional requirements document, Return On Investment (ROI) analysis, and risk assessment; and document instances where a BCA

requirement is waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements.

2. Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.

3. Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.

4. Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.

5. Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.

6. Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skills and skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.

7. Terminate efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue support for cases in progress; prepare an After Action Report that documents the problems encountered with the current software for use as input for the acquisition of a replacement contract; and initiate a new acquisition to obtain a follow-on contract using lessons learned under the current contract to avoid similar problems.

8. Develop an eDSS functional requirements document that specifies the required capabilities (including security, privacy, and performance monitoring controls), acceptance criteria, or performance characteristics of the supplies or the performance standards for the services being acquired and state how they are related to the business need; identifies requirements for compatibility with existing or future systems or programs; describes any known cost, schedule, and capability or performance constraints; and associates requirements with acceptance criteria and performance standards.

9. Require maintenance of an eDSS traceability matrix that identifies authorized functions and how they have been implemented and successfully tested. The traceability matrix should be scaled to acquisition complexity, allowing required functions to be tracked from the functional requirement document, through solicitation and acceptance testing.

10. Maintain a set of comprehensive benchmarks that can perform acceptance testing whenever the eDSS is changed; maintain a test database that will support eDSS workload analysis and troubleshooting; and use benchmark testing to establish performance baselines that can be validated throughout the eDSS contract life. Identify approaches that may be used to support stress testing analysis on a limited basis without the need to maintain a hosting facility.

11. Align a eDSS follow-on contract period of performance to allow cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

12. Prepare a Business Case Analysis that provides the rationale and support for the mobile device project and its ongoing operation; include a discussion of the risks associated with the technological model deployed; and identify system functionality and relate it to business needs.

13. Develop a System Security Plan for the mobile device project based on NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The plan should leverage the existing Data Center ATO and Maas360 PATO as appropriate.

14. Provide training in best practices for establishing and managing project schedules; ensure project schedules contain milestones for evaluating project performance; allow slack time for resolution of unintended events; and ensure that critical tasks are completed or justification is provided if project tasks or schedules are not to be completed or are delayed.

15. Identify systems that may include CUI using FTC policy effective on the date a project is submitted for approval. Include control requirements of the CUI program as identified in NIST Special Publications in FTC planning for systems, information inventories, and information protection controls. Monitor ongoing NARA and NIST CUI program activities to ensure the FTC remains current with the direction and status of CUI program requirements.[2]

[2] The National Archives and Records Administration Final Rule on Controlled Unclassified Information was published in the Federal Register on September 14, 2016, and is effective November 14, 2016. The FTC will be required to expend significant effort to comply.

Management Response and OIG Analysis of Management Response

We provided a draft copy of this report to the FTC for review and comment. A copy of management's response is included in Appendix D.

The FTC concurred with our recommendations. The FTC's response includes actions management has taken or planned to take after March 30, 2016 – the close of our data collection period. The actions management proposes to take reflect an approach that will meet our recommendation objectives. The OIG's analysis of management's response is included in Appendix E. We will examine the effectiveness of the planned improvements to the FTC's Information Technology Governance Practices as part of the OIG's FY 2017 Federal Information Security Modernization Act (FISMA) evaluation.

Table of Contents

List of Figures

Background

1. Information Technology (IT) Governance

Organizations depend on information technology (IT) to complete their business objectives and missions. IT governance is the framework that an organization uses to align its IT strategy with its business strategy and ensure that the organization meets its mission and its strategic goals and objectives. IT governance consists of the leadership, structures, and processes that enable an organization to make decisions to ensure that its IT sustains and extends its strategies and objectives.

As an integral component of enterprise governance, IT governance requires a clear understanding of the organization's strategic goals and objectives supported by a management structure with repeatable processes to support decisions that align IT investments with its goals and objectives. IT governance ensures that the FTC takes actions to ensure IT acquisition decisions:

- Identify and prioritize business needs for IT support;
- Identify risks and potential impacts from performance, security, and privacy failures;
- Review and approve strategies to align IT support to organizational goals and objectives;
- Monitor execution of plans to implement approved strategies;
- Identify when corrective action is required and monitor completion of those actions;
- Evaluate and direct the use of IT to support the organization; and
- Ensure decisions and supporting rationales are adequately documented to communicate decision objectives and provide accountability of agency personnel and contractors responsible for investment and contract execution.

IT governance is often equated with IT management. However, IT governance is broader in scope than IT management and focuses on strategically transforming and directing IT to meet present and future organizational requirements, whereas IT management focuses on the supply of IT services and products and management of associated IT operations.

IT governance has been a long-term weakness for the federal government. Congress, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) have enacted laws, policies, and guidance to establish and improve IT governance (see Appendix B). In 2011, the Government Accountability Office (GAO) identified IT governance and management as a key issue facing the United States and "identified a set of essential and complementary management disciplines that provide a sound foundation for IT management." These include IT strategic planning, enterprise architecture, IT investment management and Information Security. A recent GAO Report found that legacy federal IT investments are

becoming increasingly obsolete. The report concludes that lack of proper investment in keeping the core IT systems current will ultimately cost agencies and taxpayers both financially and in mission effectiveness[3]. GAO also concludes that more funding does not guarantee success, as upgrading and maintaining an effective and secure IT structure requires several disciplines including "project planning, requirements definition, and program oversight and governance." GAO assembled key IT governance and management best practices and offers them on its *Best Practices and Leading Practices in Information Technology Management* website.[4]

There is no single governance approach that can be applied to all organizations. Effective IT governance policies and practices are tailored to the organization's mission, culture, and technology environment.

In late FY 2011, the Federal Trade Commission (FTC) established its governance program to support planning and oversight of its IT investments. The Governance Program was defined as consisting of two bodies: (1) the Governance Board to provide a strategic, agency-wide perspective and guidance to the Commission for long-term IT investment; (2) the Technology Council (which included an IT Planning Board (ITPB) and a Configuration Management Board (CMB)) to ensure sound decision-making with input from throughout the agency with attention to life-cycle costs, information security, and enterprise architecture. The Governance Program applied to all IT applications, hardware, systems, and data investments supporting FTC business lines, processes, and/or data management activities. IT investments for new and significant upgrades to existing enterprise-wide applications or systems with life-cycle costs of $500,000 or more required Governance Board approval. Purchases below $500,000 required Configuration Management Board approval.

In FY 2012, the FTC revised its Governance structure to provide two primary Boards, a Capital Planning Governance Board and the Technology Council. The current Governance Structure (effective August 2014) is defined as three bodies: an IT Governance Board (ITGB), IT Business Council, and the IT Council.[5] Associated Governance Program policy changes included the program scope and the criteria identifying investments requiring Governance Board approval and oversight. Under the August 2014 criteria, the impact on business processes and risk of non-completion or delivery were added to emphasize the importance of organizational risk to the governance process.

For this evaluation, the August 2014 Charter was used as the program baseline. There were no identified instances where Office of Inspector General (OIG) findings or recommendations would have been different using an earlier version of the Governance Program Charter.

---

[3] Government Accountability Office, *Federal Agencies Need to Address Aging Legacy Systems* (GAO-16-696T) (May 25, 2016).
[4] Federal Trade Commission, Office of the Chief Information Officer, Information Technology Governance Program Charter, Version 1.1; January 18, 2012.
[5] Federal Trade Commission, Information Governance Program Charter, July 1, 2011 (updated August 20, 2014).

FTC Governance Program

The Scope and Principles for the FTC Governance Program are described as follows:

> To increase transparency and proactively manage risk, all IT investments are within the scope of IT governance, regardless of the estimated cost and the organization managing the investments. This includes the acquisition, development, upgrade or maintenance of all hardware, software, applications, systems, and related services investments supporting FTC business lines and management processes. While the scope of IT governance covers all types of IT investments, the level of oversight depends on type of investment and should be commensurate with its complexity and risk.

The IT governance program was implemented to –

- address weaknesses in planning for and acquiring IT capabilities that had resulted in acquisition of IT systems and contract support that did not meet FTC requirements;

- establish an agency-wide, risk-based framework for acquisition and management of IT investments that complies with federal requirements and provides the FTC with the IT resources it requires; and

- ensure that performance of IT investments can be effectively monitored and managed.

Key components of the FTC Governance Program are the Governance Boards. The Charter established three interrelated entities that are collectively responsible for development, management, and operation of the IT Governance Program. These Boards and their responsibilities are summarized as follows:

- **IT Governance Board** (ITGB) serves as the top-level component of the agency's overall IT governance structure. The ITGB provides high-level guidance on overall IT objectives and strategic priorities; approves the agency-wide IT Portfolio; and reviews and makes significant IT investment selection and control decisions. The ITGB votes to approve/disapprove with conditions Full Business Cases.

- **IT Business Council** (ITBC) serves as a precursory, recommending body to the ITGB. The ITBC conducts in-depth reviews of strategic plans, proposed agency investment portfolios, and the status of existing portfolios as drafted by the ITC. Once plans and portfolios are reviewed, the ITBC makes recommendations to the ITC for changes as necessary. The ITBC makes recommendations to the ITGB on drafted strategic plans, investment portfolios and portfolios, and proactively identifies investment risks.

- **IT Council** (ITC) serves as a precursory, recommending body to the ITGB and ITBC. The ITC serves as the business unit's point of contact for all proposed investments. The ITC works with business units to develop, support, and complete business cases and market research commensurate with the level of investment.

As described in the IT Governance Program Charter, the primary decision document in the Governance Program is the Business Case Analysis (BCA). A Business Case Analysis is not required for every investment for "Steady State" Operations and Maintenance (O&M), and an operational analysis is completed "as needed." A Business Case Analysis is required for all Development, Modernization, and Enhancement (DME) investments. At a minimum, a Business Case Analysis must contain an executive summary that provides a high-level view of the project. The executive summary explains the project and its goals in concise and plain language. A full Business Case Analysis is required for investments with a –

- Five-year life cycle cost ≥$1M;
- High-impact on business processes; or
- High-risk of not completing execution and delivery.

The Business Case Analysis describes the business need and provides support for approving IT investments. The FY 2011 Charter described a Business Case Analysis as containing -

- A Statement of Purpose: A Requirements Analysis or a Situation Description;
- An Analysis of Alternatives: A description of alternative options and possible solutions, including taking no action, and the risks and benefits of each option;
- A Life-Cycle Cost Analysis: A synopsis of the life-cycle costs and ROI or a justification of estimate (JOE) for each option, including the proposed solution; and
- An Implementation Plan: A high-level timeline to implementation, noting major milestones.

In practice, the FTC had two types of Business Case Analyses: an abbreviated Business Case Analysis for small investments with little complexity and a full Business Case Analysis for all other investments. In response to an OIG recommendation, the two-level Business Case Analysis process was formalized as an Executive Summary Business Case Analysis and a Full Business Case Analysis in the August 2014 Charter. The full Business Case Analysis expands on the executive summary and provides additional details. Development of Business Case Analysis Templates and instructions are the responsibility of the IT Business Council. Appendix C provides the templates for the Executive Summary and Full Business Case Analysis.

Whereas the Business Case Analysis is identified as the primary decision artifact in the Governance Program Charter, the *Office of the Chief Information Officer (OCIO) IT Acquisition Strategy* identifies the Acquisition Plan as the primary artifact for all FTC contract acquisitions. The Acquisition Strategy defines how the Federal Acquisition Regulation (FAR) is interpreted at the FTC for IT acquisitions.

Both the Business Case Analysis and the Acquisition Plan must be addressed for FTC IT projects or acquisitions; the topic areas for a BCA are also topic areas for an Acquisition Plan, and both the Acquisition Plan and Business Case Analysis require that projects and acquisitions have a business need-to-requirement linkage. The Acquisition Strategy defines a process for conducting IT acquisitions / investments that aligns with FAR requirements for acquisition planning and management. The information elements for an FTC Business Case Analysis are a subset of the Acquisition Plan elements. Thus, each Business Case Analysis element has an equivalent in the Acquisition Plan. Acquisition Plan elements, however do not all have a corresponding Business Case Analysis element. [6]

In accordance with the Federal Information Security Modernization Act (FISMA), the FTC OIG conducts an annual independent evaluation of the status and effectiveness of FTC security and privacy programs, under guidance developed by the Department of Homeland Security (DHS) and policies promulgated by the Office of Management and Budget (OMB). A critical element of this annual evaluation is an assessment of the FTC IT Governance Program. The assessment seeks to determine if the IT Governance Program provides the framework needed to ensure that FTC IT investments are providing effective, secure IT systems that meet FTC business objectives.

Since FY 2011, the OIG has provided recommendations to address identified weaknesses in FTC IT governance processes. Among these recommendations were:

- FY2011 – 02: Risk Management – FTC needs to implement a risk management program compliant with NIST SP 800-39;

[6] For example, the template for a Full Business Case Analysis request consideration of project risk in three areas: implementation risk relative to analysis of alternatives, Privacy and Security Risks which focuses on PII, and Analysis of Other Risks such as cost, schedule, scope, technology, and management. The requirement to analyze risk is described in FAR Part 7.105 as –

> (7) Risks. Discuss technical, cost, and schedule risks and describe what efforts are planned or underway to reduce risk and the consequences of failure to achieve goals. If concurrency of development and production is planned, discuss its effects on cost and schedule risks." Which is augmented by FAR 39.102 Management of risk which is specific to IT acquisitions.
>
> (a) Prior to entering into a contract for information technology, an agency should analyze risks, benefits, and costs. (See Part 7 for additional information regarding requirements definition.) Reasonable risk taking is appropriate as long as risks are controlled and mitigated. Contracting and program office officials are jointly responsible for assessing, monitoring and controlling risk when selecting projects for investment and during program implementation.
>
> (b) Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high risk projects to be monitored, funding availability, and program management risk.
>
> (c) Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures.

- FY2011 – 11: Implement Capital Planning for HSPD-12 Acquisitions –FTC needs to institute a capital planning program on an accelerated basis and include acquisitions currently in process.

- FY 2012 – 01: Risk Management/ Management Structure

    - Include risk as a factor in determining when IT review procedures apply.
    - Implement a risk management program compliant with NIST SP 800-39.

- FY 2012 – 02: I&A Management – FTC IT governance boards should receive regular progress reports on all board approved projects.

- FY 2012 – 08: Privacy – FTC POAM process should include Privacy Steering Committee (PSC) initiatives that affect NIST SP 800-53 controls.

- FY 2013 – 01: Risk Management/Management Structure

    - Continue implementation of a risk-based governance structure that is applied to all IT investments and initiatives.
    - FTC needs to implement a NIST SP 800-39 compliant risk management program.
    - FTC should implement an Information Security Continuous Monitoring (ISCM) program using its governance process and incorporate in place components.

- FY 2014 – 01: Security Management Structure
    - Continue to evolve FTC governance practices and expand the use of CPIC and investment analysis processes to document investment decisions. Ensure that risk-based decisions are appropriately documented for input to Information Security Continuous Monitoring (ISCM) reporting.

- FY 2014 – 02: Risk Management / Management Structure

    - FTC should accelerate its implementation of NIST SP 800-39 compliant risk-based governance and IT investment processes. These processes should be applied to the FTC IT modernization effort and its associated activities.

- FY 2015 – 01: Security Management and Governance Structure

    - Continue to evolve FTC Continuous Monitoring Management practices through improvements in governance practices and providing improved documentation and estimating guidance.
    - Review governance policies and procedures to resolve potential organizational conflicts of interest and confusion in roles and responsibilities, and ensure that

Boards are appropriately established and resourced and its processes sufficiently guided and documented to complete assigned responsibilities.

- FY 2015-04 to elevate the Chief Privacy Officer to voting membership on the ITGB.

The OIG's consistent identification of IT Governance Program weaknesses also showed that while the program is improving, there remain significant opportunities to accelerate maturation of the Program. Consequently, the OIG contracted with TACG, LLC to evaluate the FTC's IT Governance Program with a focus on project review and approval. TACG performed this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* promulgated in January 2012 by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The data collection period commenced on July 24, 2015, and concluded on March 30, 2016.

In addition to evaluating FTC IT Governance Program policy and procedural documents, TACG identified two projects that the Governance Board had identified as problem projects in Governance Board materials. These projects had been approved and monitored through the FTC Governance program. These programs were added to determine if Governance Program weaknesses were contributing factors to the project deficiencies. In addition, the new government-wide Controlled Unclassified Information (CUI) Program was added to the evaluation. TACG added the CUI program to evaluate how the FTC is incorporating new program guidance with potential long-term Information System impacts into FTC planning.

2. CIGIE Maturity Model

In FY 2015, DHS changed its evaluation methodology to incorporate a "maturity model" approach. Under this approach, DHS defines performance criteria for specific program stages where the level of security/privacy risk decreases as an agency program matures. In its FISMA reviews, the OIG now evaluates FTC security and privacy programs to determine which stage of development the agency has achieved and provides recommendations to mitigate identified weaknesses.

Working with the CIGIE, DHS plans to define maturity stages and associated performance criteria for each of ten FISMA topic areas (Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones, Remote Access Management, Contingency Planning, and Contractor Systems -- subsequently consolidated to five domains (Identify, Protect Detect, Respond, Recover) in FY 2016 reporting guidance). In its FY 2015 reporting guidance, DHS provided maturity model criteria for the Continuous Monitoring Management (CMM) topic. CMM ensures that the agency Information System Continuous Monitoring (ISCM) program is properly established, is providing effective security, and includes consideration for evaluating the effectiveness of the FTC IT Governance Program. In FY 2016, use of the CIGIE scale will be expanded to all domains evaluated.

The CIGIE maturity model provides evaluation criteria for three analysis areas (People, Processes, and Technology) and five performance levels (1-Ad-hoc, 2-Defined, 3-Consistently

Implemented, 4-Managed and Measurable, and 5-Optimized). In FY 2015, the OIG assessed the FTC Governance Program using the CIGIE performance levels and FY 2015 data. The OIG's assessment showed that the FTC IT Governance Program is operating at performance Level 2, meaning that policies are defined and are disseminated throughout organization, but the program is inconsistently applied.

Why We Did This Review

In accordance with federal policy, the FTC Governance Program provides an agency-wide accountability framework for IT investments. All FTC IT investments are subject to review and approval under the FTC Governance Program, including the acquisition, development, upgrade or maintenance of hardware, software, applications, systems, and related services investments supporting FTC business lines and management processes. The Governance Program has a critical role in planning, monitoring, and managing FTC IT capabilities.

FTC employees and contractors depend on IT systems with support provided by the FTC's Office of the Chief Information Officer (OCIO) to complete their tasks, whether these tasks are administrative or in fulfillment of the competition or consumer protection mission executed by the FTC's Bureaus and Offices. These tasks include FTC litigation support and program activities, such as the National Do Not Call Registry, privacy, electronic commerce, consumer protection, and competition work. The general public also relies on these resources to file consumer complaints, submit pre-merger filings, and interact with the FTC's other activities and programs. As described more fully below, FTC data repositories contain Personally Identifiable Information (PII) protected by federal privacy laws, and highly sensitive market and pricing data filed by entities seeking merger or acquisition approval that iscategorized as Controlled but Unclassified Information. The FTC's IT systems secure the data held in these repositories and provide the platforms that enable FTC staff to use that and other data sets in conducting FTC litigation and other core mission tasks. The FTC IT Governance Program provides a management framework to ensure that FTC IT assets (hardware, software, information) are adequately protected, available when needed, and provide the support needed to successfully perform its multiple missions.

FTC IT capabilities are provided through a mix of legacy and state-of-the-art technologies that were largely acquired to address immediate needs, with limited long-term, enterprise-wide planning. For example, FTC IT support focuses on individual projects or investments and has not yet developed an Enterprise Architecture with associated priorities and risk thresholds to ensure that needed IT capabilities are provided across the FTC efficiently, securely, and consistently.

The FTC is currently conducting a multi-year effort to modernize its IT capabilities. Current planning includes initiatives for the following investments: (1) upgrading the network to provide stability and increased security; (2) providing building-wide wireless access at the headquarters and regional offices; (3) continuing mobile device management and modernization; (4) managing website hosting, Lexis Nexis, and Westlaw contract recompetes; (5) moving to an external cloud-based email-hosting provider, with a more secure, scalable, reliable, and efficient platform; (6) deploying a fully functional enterprise content management system (ECMS); (7) replacing the Matter Management System 2; (8) upgrading the e-Filing system; (9) improving

e-Discovery tools; (10) enhancing the Secure Investigation Laboratory; and (11) automating filings. The modernization efforts provide for planned IT investments of more than $24 million from FY 2015 through FY 2017 ($4,645,000 in FY 2015, $8,014,000 in FY 2016, and $12,064,000 in FY 2017).

In addition, agency program managers monitor and maintain automated systems and databases that collect, track, and store performance data. As noted in the FTC's FY 2016 and 2017 Performance Plan, the Office of the Chief Information Officer (OCIO) has launched a number of information technology initiatives to protect the agency's networks, systems, and data from compromise and loss. This plan also indicates a specific performance goal that monitors the availability of these mission-critical IT systems, such as email, telecommunications, Internet access, and mobile devices.

With FTC employees and stakeholders critically dependent upon IT systems, effective IT governance is crucial to ensure that IT resources are in place to support its core missions. Weaknesses in IT governance can result in systems that do not perform needed functions, are costly to operate and maintain, and increase security risks. By contrast, mature IT governance ensures that performance and security risks are minimized as the FTC adopts new technologies and technical approaches to improve service to its stakeholders, including the general public. For example, there are significant external pressures to replace in-house computing facilities with cloud-based solutions. Using cloud-based services can reduce operating costs while increasing system availability. However, introducing this type of major technology change also changes the agency's risk profile (i.e., commercial cloud systems have different risks than the FTC's in-house data center).

The OIG's FY 2015 FISMA evaluation assessed that the IT governance program and its associated Information Security Continuous Monitoring (ISCM) program are performing at Maturity Level 2: policies are defined and are disseminated throughout the organization, but the program is inconsistently applied. The evaluation also identified significant, mission critical projects where governance deficiencies resulted in delivery of IT services that do not meet the needs of the FTC workforce, are not effectively monitored to ensure adequate performance, and are not auditable such that decisions and the authority and rationale for those decisions cannot be determined.

1. Authority

A number of Federal laws, policies, regulations, and standards set forth the requirements for effective planning, acquisition, oversight, and monitoring of IT investments. They include the following:

- Federal Information Security Modernization Act of 2014 (FISMA)
- Office of Management and Budget (OMB), Circular A-130: *Management of Federal Information Resources* (11/28/2000)
- OMB Circular A-130: *Managing Information as a Strategic Resource* (7/28/2016)
- OMB Circular A-123: *Management's Responsibility for Enterprise Risk Management and Internal Control*
- National Institute of Standards and Technology (NIST)

    - Special Publication NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
    - NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

- Federal Acquisition Regulation (FAR) – (Subpart 7.1—Acquisition Plans)
- Acquisition policies and procedures for use in acquiring—

    - (a) Information technology, including financial management systems, consistent with other parts of this regulation, OMB Circular No. A-127, Financial Management Systems and OMB Circular No. A-130, Management of Federal Information Resources.
    - (b) Information and information technology.

- FTC Information Technology Governance Program Charter
- The Federal Trade Commission, Office of the Chief Information Officer, *Acquisition Strategy for Information Technology*, September 2011

2. FTC Strategic Plan and Objectives

The IT Governance Program is established to meet the following FTC strategic objective:

- FTC Quadrennial Strategic Plan (2014 – 2018): Objective 3.1 Optimize resource management and infrastructure. Supporting the mission –

    Ensuring that the FTC has effective information technology (IT) infrastructure is vital to meeting the Commission's strategic goals. The Office of the Chief Information Officer delivers value by identifying and providing a host of critical high quality, low-risk IT services that are agile enough to meet Commission business needs.

    The FTC believes in the importance of accountability and transparency, as shown through resource stewardship and financial oversight activities. The work in this area covers a wide range of administrative and operational efforts, such as formulating and executing the agency budget, managing acquisition activities, overseeing the internal control program, managing accounting operations, spearheading audit resolution, and ensuring compliance with financial management laws and regulations.

To achieve the Commission's strategic objectives, the IT governance program must provide a common structure for selecting and managing IT investments to ensure effective support to FTC operations and programs, minimize risks, and enable effective oversight.

Purpose, Scope, and Methodology

This evaluation identifies areas of weakness for correction and opportunities to accelerate maturation of the FTC's IT Governance program, using FISMA performance criteria. The evaluation included analysis of the IT Governance Program and supporting management artifacts, including the Program Charter, selected Business Case Analyses, Meeting Minutes, TechStat documentation, acquisition artifacts, project planning documents, and Project status reports.[7] The reviewers interviewed key FTC staff to augment evaluation of review areas where documentation was not available or was deficient.

The assessment methodology entailed close analysis of three IT projects, using documentation customarily developed as part of FTC's normal acquisition operations. The selected projects met the dollar value criteria for compliance with the FTC Acquisition Strategy for Information Technology (i.e., Five-year life cycle cost ≥$1M, High business impact, High potential for not meeting project objectives or costs):[8]

- e-Discovery Support System (eDSS) – The eDSS is a project initiated in 2011with an estimated 5-year cost of between $4 million and $5 million, an initial contract award of more than $6 million with a current total life cost of more than $9 million, to replace and modernize FTC software tools used in support of FTC litigation activities and other intensive analysis of large volumes of information. Information collected during the OIG's FY 2015 FISMA evaluation showed that the eDSS was a troubled project, experiencing schedule delays and cost overruns, was not delivering required

[7] A TechStat is a face-to-face, evidence-based review of an IT investment that is used to evaluate and identify the root causes of an underperforming project. A TechStat includes objectives and metrics used to monitor performance against those objectives; identifies the cause of poor performance and next steps for their resolution; and includes a corrective action plan for tracking actions to completion.

On December 9, 2010, the Federal CIO released the *25-Point Implementation Plan to Reform Federal Information Technology Management*. The plan established the requirement for Federal agencies to establish TechStat sessions on troubled investments on an on-going basis at the department level by March 2011. The plan also called on CIOs to expand TechStat sessions to the bureau-level within agencies by June 2012.

[8] FTC policy and the FAR require that an Acquisition Plan be developed and maintained for development programs or support services meeting the following criteria:

- Development programs, as defined in Federal Acquisition Regulation (FAR) 35 .001, with an expected total cost of all contract line items estimated at $1 million or more in modernization, enhancement, development, test, and evaluation.
- Production programs and support services acquisitions (including contractor services that provide assistance to a program office or functional organization in supporting systems or programs) with a total cost of all contracts estimated at $1 million or more for all years of the program, or $1 million or more for any one fiscal year.

functionality. Governance Board minutes began to document eDSS performance problems in January 2014;

- Messaging Infrastructure Modernization Project/ Mobile Device Management (mobile device project) – The mobile device project (with an estimated cost between $8.9 million and $12.9 million over 5-years) was initiated in May 2014 to modernize FTC Email/Collaboration capabilities, Mobile Device Management, and Wireless Services. A key objective of the mobile device project was to replace the FTC's aging Blackberry email and telephone service with state-of-the-art "smart phones;" and

- Controlled Unclassified Information (CUI) program – The CUI program may impact FTC information systems, particularly in data labeling and information ownership tracking. Also, CUI security guidance by the National Institute of Standards and Technology (NIST) is defining new or revising existing controls that FTC information systems must address (e.g., NIST SP 171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, issued in June 2015 and updated January 2016, affects FTC plans to systems move from the FTC Data Center to commercial hosts). The National Archives and Records Administration (NARA) is establishing a CUI categorization taxonomy that may require system design changes.

  The FTC collects a large volume of sensitive, unclassified information. Under the CUI program established by NARA in accordance with Executive Order 13556 (Nov. 4, 2010), all such information must be uniformly designated as CUI. Currently, there are 23 broad categories of CUI, which are further divided into subcategories. The FTC has CUI in several of these categories or subcategories, such as Financial-Mergers (i.e., HSR data), Information Systems Vulnerability Information (i.e., FISMA, 44 U.S.C. 3545(f)), Legal-Administrative Proceedings (i.e., *in camera* material under Rule 3.45), Legal-Privilege (i.e., Fed. R. Civ. P. 26 in Federal court proceedings), Legal-Protective Order (i.e., protected by section 21 of the FTC Act, 15 U.S.C. 57b-2), Privacy (i.e., Privacy Act of 1974, 5 U.S.C. 552a), and Proprietary Business Information (i.e., section 6(f) of the FTC Act, 15 U.S.C. 46(f)).[9] The FTC can estimate its CUI holdings in total and uses

[9] In May 2008, the White House issued a memorandum to initiate a program to consolidate all designations for sensitive but unclassified terrorism information into a single category designated, Controlled Unclassified Information (CUI). The Memorandum designated NARA as the Executive Agent (EA) responsible for managing and overseeing implementation of a program to establish a single set of policies to ensure the consistent designation, marking, safeguarding and dissemination of terrorism-related CUI. (The designation change to CUI was accompanied by a new and separate program to reduce CUI holdings similar to ongoing OMB efforts to require that Federal agencies review and their volume of sensitive information PII holdings. *See, e.g.*, OMB Memorandum M-07-16 (May 22, 2007) at Att. 1, sec. B.1. Current and forthcoming CUI guidance also links the CUI requirements to the policies and procedures issued by NIST for ensuring information security and privacy under FISMA. The CUI program has since been expanded by the 2010 Executive Order, *see supra*, beyond terrorism-related CUI to all unclassified information requiring safeguarding and dissemination controls by law, rule, or policy.

that information in monitoring its holdings of sensitive information. Until the CUI definitions are finalized, the FTC cannot formally distribute its CUI holdings across the 23 categories, and more than 85 subcategories. However, as noted above, the FTC has identified CUI holdings in three broad categories that are included in the CUI program: 1) proprietary business information, such as trade secrets and highly sensitive market and price data provided to the FTC as part of merger or acquisition filings; 2) information obtained pursuant to law enforcement actions or proceedings, which can include international matters; and 3) PII pertaining to consumers, employees, or other individuals. In these areas, the FTC is obligated not to disclose such information, without authorization, and must provide appropriate safeguards in accordance with requirements established by the information owner. Further, other agencies that share data with the FTC may assign information to different CUI categories. The FTC must be capable of handling information received in accordance with applicable law and as specified by the information owner. The level of effort that may be required to bring FTC systems into compliance with the forthcoming final requirements for the proper marking and safeguarding of CUI is uncertain, but prudent planning practices should include potential CUI impacts as a risk item.

Results of the Review

In two of the three projects evaluated, the OIG identified systemic weaknesses in project planning and monitoring that hinder security/privacy program maturation. These weaknesses resulted in delivery of products and services that do not meet FAR and FTC requirements. To date, planning and monitoring deficiencies for the eDSS and mobile device project resulted in increased acquisition costs and operations and maintenance (O&M) costs and in decreased program effectiveness and system usability. Fortunately, information security and privacy were not affected due to compensating countermeasures within the FTC's security control environment. However, reliance on these measures increases staff workloads and stress, introduces security and performance risks, and is not sustainable.

Correction of systemic weaknesses and implementation of continuous process improvement will accelerate maturation of the FTC Information Security Continuous Monitoring (ISCM), allowing FTC to progress from Level 2 of the CIGIE maturity 5-level model to Level 3, and ultimately achieving Levels 4 and 5. The maturation from Level 2 to Level 3 is critically important: Level 2 maturity shows that the FTC understands that effective security and privacy requires defined, appropriate policies and procedures. Level 3 maturity shows that the FTC consistently applies its security and privacy policies. Thus, a Level 3 provides the maximum impact on the FTC's ability to protect its information assets. Levels 4 and 5, while important to process maturity, and focus on monitoring and improving the ISCM, primarily affect the FTC's ability to adapt its ISCM to technological and mission changes.

1. Failure to follow FAR Business Case Analysis/Acquisition Planning guidance resulted in increased costs and diminished performance

The FTC uses the FAR to obtain systems and services necessary to maintain the secure, reliable information systems critical to performance of its multiple missions. The FAR defines "acquisition" to mean:

> the acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

The FAR defines acquisition planning as "the process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition." An Acquisition Plan (AP) is the comprehensive plan identified in this definition.

The FTC developed an OCIO IT Acquisition Strategy that parallels FAR acquisition requirements, but tailors requirements to the FTC environment. In the 2011 OCIO IT Acquisition strategy, the Business Case Analysis is analogous to the FAR Acquisition Plan. The FAR and the OCIO IT Acquisition Strategy provide similar detailed structures and contents of an Acquisition Plan/Business Case Analysis for planning and monitoring significant acquisitions (acquisitions with a total acquisition cost of $1million or more). The FTC IT governance policy extends acquisition planning to projects with potential security or privacy risks.

FAR and FTC planning requirements are expected to be tailored to specific project requirements based on cost, project complexity, and risk. However, the FTC did not follow this guidance in two of the three projects evaluated by the OIG (eDSS and mobile device projects), and planning for the third – integration of CUI into FTC long-term planning – is showing characteristics of planning weakness. For example, NARA guidance will have a significant impact on handling and reporting of CUI incidents, but the impact of such changes are not reflected in the FTC's system modernization planning.

The following sections describe the project planning weaknesses and one project monitoring weakness identified by the OIG in the eDSS and mobile device projects.

a. Statement of Need did not demonstrate a supporting business rationale

Acquisitions need to relate the IT requirement to a business need in conjunction with a description of similar prior acquisitions and alternatives that might provide feasible alternative solutions. The FAR describes a Statement of Need as follows:

> **Statement of need**. Introduce the plan by a brief statement of need. Summarize the technical and contractual history of the acquisition. Discuss feasible acquisition alternatives, the impact of prior acquisitions on those alternatives, and any related in house effort. (FAR 7.105 (a) (l))

The November 2011, the eDSS Business Case Analysis addressed this requirement with a statement that the tools then in use were no longer adequate to support FTC litigation support efforts. It included an extended description of the Electronic Discovery Reference Model

(EDRM) and various approaches for acquiring the needed capabilities (e.g., licensed software hosted internally, software as a service with remote hosting, and modular acquisitions). The Business Case Analysis explicitly omitted a cost benefit analysis showing current usages and costs versus expected changes in usage and costs with a replacement system. Thus, the Business Case Analysis effectively sought funding for a project without the information necessary to estimate the reasonableness of requested funding or to evaluate the potential for successful completion.

The mobile device project had no formal Business Case Analysis. The project was initiated with a needs analysis and a market survey that encompassed the totality of the FTC mobile messaging needs. The presentation to the Governance Boards and the Chairwoman consisted of information collected through the needs analysis and a market survey. While the briefing document was treated as a Business Case Analysis, it did not contain significant items required by the FAR and FTC policy for a project of the size (more than $1 million total cost) and complexity of the mobile device project or its smart phone replacement component. For example, the Business Case Analysis did not include a System Security Plan or a functional requirements document. The functional requirements document (FRD) is a formal statement of an application or systems functional requirements.[10] The lack of formal planning resulted in delays and disruptions in deployment of the mobile device project.

FAR guidance states that Acquisition Plans should be revised over time to reflect changes in the acquisition strategy and completion of plan activities. This information facilitates monitoring by the Governance Boards and FTC management. The FAR and the OCIO Acquisition Strategy require that project plans include milestones to ensure that the acquisition plan is updated. We found that the eDSS and mobile device project Business Case Analyses did not address plan maintenance or include update milestones. Thus, the Acquisition Plan was not regularly updated, at least annually, as recommended by the FAR.

b. Acquisition Plan/Business Case Analysis did not address all applicable conditions

An Acquisition Plan should discuss all significant, applicable conditions that may affect the scope, performance, and risk associated with an acquisition. This would include increased security requirements, the environment in which a system is to operate, and the need to maintain compatibility with legacy systems. Both the eDSS and the smart phone Acquisition Plans omitted presentation of significant conditions that adversely affected performance, system utility, and user satisfaction:

- eDSS – The eDSS Business Case Analysis did not describe FTC security requirements specific to its litigation support and mergers and acquisitions activities. For example, eDSS planning documents did not address security requirements (i.e., a security baseline

[10] A functional specification in systems engineering and software development is a document that specifies the functions that a system or component must perform (often part of a requirements specification) .

was not provided) and the need to sequester (isolate) information erroneously produced to the FTC to avoid inappropriate access and use. The sequestration issue necessitated an FTC-funded, unplanned development effort after contract award (December 2013) to modify a commercial product to provide the needed capability.[11] Similarly, the eDSS Business Case Analysis did not identify or describe the need to maintain compatibility with legacy file systems, although such compatibility was listed as an eDSS functional requirement.

- Mobile Device Project – The mobile device project Business Case Analysis omitted the information needed to identify the risks and solution characteristics associated with the deployment of multi-purpose smart phones to replace its obsolete Blackberry environment (e.g., a need for certificate-based security, providing service in the wireless-isolated Constitution Center, and supporting FTC staff on international assignments). This omission was complicated by a failure to prepare a System Security Plan, as required by FTC policy. A System Security Plan would have identified most of the omitted information.

c. Life-cycle cost analyses were deficient

The FAR requires that information technology acquisitions analyze associated risks, benefits, and costs.[12] Cost benefit analyses such as a Return On Investment (ROI) analysis were not performed for the eDSS because, per the Business Case Analysis, "all of the cost data for the current system is unknown." Instead, the Business Case Analysis provided a cash flow model that showed how planned spending or available budget might compare against three alternative solutions. The cash flow technique used showed estimated spending patterns that were not tied directly to cost. Further complicating the analysis was an assumption that all estimates are Rough Orders of Magnitude (ROM), which means that the estimates have significant variability and, per GAO recommendations, should not be used for budget quality decisions.

Given the characteristics and reliability of the Business Case Analysis cost data, the attestation that the Business Case Analysis cost estimates are reasonable has a high risk of failure: the cost data are highly variable rough order of magnitude spending patterns -- not cost estimates -- and the current comparative cost baseline uses data characterized as unknown. Thus, the eDSS cost estimate for the multi-year effort of between $1.3 million and $ 1.5 million for year 1, with a 5-year estimated cost ranging from $4.4 million and $ 5 million has a high probability of failure. The current estimated completion cost is $7.9 million.

Unlike the eDSS, costs for the mobile device project showed an understanding of the cost elements and projected volumes. While no cost benefit analysis was performed during the Business Case Analysis process, this deficiency did not have a material impact on project cost

[11] At its December 2013 meeting, the Technology Council and Governance Board approved spending an additional $139,724 so that a custom sequestration or "clawback" solution could be created and implemented.
[12] FAR Section 39.102, Management of Risk.

analyses because smart phones have become commodity purchases. Price reasonableness is maintained through competition and determined by the General Services Administration (GSA). That said, the absence of a cost benefit analysis eliminated an opportunity to determine whether a two-instrument solution provided a greater ROI than a single instrument solution

d. Design-to-cost assumptions were incorrect

Both the eDSS and the mobile device projects identified commercial products and services as the desired solution for FTC business requirements, a decision that would have precluded the need for a design-to-cost analysis. This was an incorrect assumption for the eDSS. As described in the Business Case Analysis, there was likely no single solution to the FTC EDRM requirement. Given that it would be unlikely that a single commercial, off-the-shelf solution was available, the low-risk approach would be to assume that some level of product development or modification would be required to provide the capability to move or share data between multiple applications. Using the low-risk approach, the FTC would have been able to include development efforts as part of the eDSS solicitation, providing offerors an opportunity to describe a solution and associated cost for providing a tool to facilitate data sharing between multiple products. This conclusion is supported by post-award FTC actions to modify the selected product to provide needed functionality, such as sequestration of litigation data incorrectly provided to the FTC and the identified need for system modifications for appropriate audit and performance data.[13]

The mobile device acquisition used commercial, off-the-shelf software and systems. This approach required that any selected solution would need to be specifically configured for the FTC environment. Per NIST guidance, such configuration artifacts are components that should be identified in the associated System Security Plan. The mobile device project plan provided time and resources for configuring and documenting the solution. However, the FTC understated these estimates because the level of effort required to establish a certificate-based access control environment was greater than anticipated. The anticipated level of configuration and testing would not trigger a need to develop a design-to-cost assessment because no program software changes are required.

e. eDSS did not include a "should-cost" model

The FAR requires development of a "should-cost model" for acquisitions. A should-cost model provides the organization's best estimate of the full cost of the acquisition. A full cost estimate should include a Basis of Estimate (BOE) that explains how the estimate was developed, identifies any assumptions or constraints affecting the estimate or its use, and describes estimate variability (e.g., identifies volume-sensitive pricing). The should-cost model provides the basis

[13] The FTC encountered a similar problem when trying to evaluate product performance. The acquired product did not have the capability to collect user-focused performance data that would allow evaluation of product performance at varying system workloads. The system changes to remedy this deficiency were estimated, but not authorized, as the FTC determined that such changes would not be cost effective because the contract was reaching the end of its period of performance.

for the Independent Government Cost Estimate (IGCE) that is used as the basis for a cost/benefit analysis or a ROI, and to evaluate price proposals.

The eDSS Business Case Analysis did not include a should-cost model. Instead, the Business Case Analysis presented a cash flow model that showed expenditure flows, but provided little information about expenditure effectiveness, or whether the cash flow was for full or partial funding. It, therefore, was not a viable technique for evaluating pricing models. Further, the eDSS Business Case Analysis cautioned against reliance upon the estimates provided as they were ROMs, did not include all costs, and did not include volume sensitivity analyses.

The lack of reliable cost/price estimates and volume sensitivity analysis increased the risk of budget overruns and schedule delays due to inadequate funding. The Business Case Analysis cost estimate for the eDSS project was $5 million. The current completion estimate at completion is $7.9 million, an estimate overrun of more than 50%.

While the mobile device project Business Case Analysis did not provide a price analysis, the pricing provided was approached on a should-cost basis. The should-cost pricing provided a reasonable basis for analyzing proposed pricing and project management. There were no significant delays or budget deficiencies attributable to the mobile device project price/cost analysis.

f. Inadequate functional requirements

As noted above, FAR states that an acquisition plan should specify the goods or services sought in a manner that is sufficient to support the Business Case Analysis through the approval process. For the eDSS, the functional requirements should be based on the required system capabilities and should state whether the function is currently in use, is a new functional requirement, or is a desired function. The functional requirements analysis should also link to a description of the requirement, criteria for successful performance, and procedures for performance testing.

Both the eDSS and mobile device Business Case Analyses had deficient functional requirements. eDSS had a list of functions that the system was to provide, but there was no discussion describing the functions and associated performance criteria.

The deficient functional requirements caused challenges for both eDSS and the FTC-issued mobile devices.

- The eDSS was electronic document review software intended to replace Concordance as well as some of the functionality of other legal processing and review tools. There were problems with the implementation, given that the installation coincided with the staff move to Constitution Center. There was also a "rocky" software deployment; OCIO needed months to fix the problems.

  In choosing software, the FTC underestimated how much adaptability the Bureaus would need. The FTC thought the agency would adapt the software to the business processes, as opposed to the reverse.

In one period during June and July 2015, extreme latency in the network severely impeded work of the Bureaus of Competition and Consumer Protection. The latency resulted from an application flaw that the contractors fixed: the software was not properly configured, and so the cache was larger than the configuration. As a result, attorneys had a difficult time extracting documents to prepare for upcoming hearings. Afterward, the OCIO increased resources to evaluate and analyze the environment and implement necessary configuration changes.

- As for the mobile devices, the functional requirements deficiency resulted in delayed implementation of a smartphone mobile device platform as well as configuration and integration issues with the agency's legacy email and identity management platforms. End users encountered difficulty with signal strength, connecting to wireless networks, browser issues, and trouble with native applications. These difficulties were largely resolved prior to and during deployment.

While FTC testing and product demonstrations were performed as part of the eDSS solicitation, all critical functions were not analyzed or tested in a manner that demonstrated scalability as well as functionality. Without scalability testing, the FTC accepted the high risk that the system would fail as the workload volume or number of concurrent users increased. Performance risk was also increased by the contractor selection approach. The eDSS contract was awarded on a "Best Value basis," where the offerors were "evaluated based on customer satisfaction, quality, timeliness, cost control, and business relations." These criteria omit an objective assessment of performance risk, which includes the capability of the offeror to deliver a solution that meets functional requirements and can effectively scale to address changes in the number of concurrent users and workload variations, such as spikes and surges.[14]

The lack of a functional requirements document also adversely affected the mobile device project. For example, the functional requirements included deployment and support for two telephone instruments. However, there was no supporting rationale for a two-instrument solution. The two-instrument solution resulted in increased project costs and schedule delays.[15] Similarly, failure to identify the need for international support for FTC staff on travel, and the complexity of certificate-based network access control, also resulted in schedule delays.[16]

Some of these adverse impacts might have been resolved through the planned technical and customer pilots (e.g., lack of WIFI coverage, omission of service for international travelers, and administrative issues associated with management of security certificates). However, the FTC

[14] A spike is a short-term, transient workload increase such as the FTC might encounter when required to perform additional analysis to support a discovery question from a defendant. A surge is a longer term workload increase such as a workload increase resulting from initiation of a complex, large case.
[15] Increased cost is demonstrated by redundant activities in the project plan for the two selected smart phones.
[16] Governance Board minutes reflect the schedule delays and user inconvenience impacts resulting from omission of international travelers, but overlooked the effort required to install certificate-based security. Certificate-based security means that every site authorized for FTC access must have an independent certificate that identifies the site and its owner, as does every instrument that is authorized to use that site. The effort to acquire, install, and maintain certificates is significant.

elected to move toward full deployment without completing the associated reporting and findings resolution.

g. Delivery or performance-period requirements were not discussed

FAR provides that the performance period for an acquisition should be aligned with business needs. Larger contracts typically warrant longer periods of performance to reduce the cost of acquisition relative to project costs; projects with cyclical workloads may benefit from periods of performance that align with those workloads; and periods of performance may be overlapped between contracts to provide for extended periods to smooth transitions between contract/product changes.

eDSS did not include a discussion of performance period versus business needs. Instead, contract performance periods are based on budget timeframes and customary transition periods (i.e., five-year contracts with a transition in and a transition out). eDSS is a capability required to support FTC's dual mission of protecting consumers and promoting competition. The capability is used by almost all FTC Bureaus and Offices. The FTC cannot afford the business disruptions that result from switching between products. For example, the current eDSS contract has a five-year performance period, with one-year transition periods. Thus, as planned, the current eDSS contract anticipated a best case product useful life of three years for a mission-critical capability. This is a high-risk planning horizon for an FTC core support requirement.

The FTC should be using acquisition flexibility to tailor requirements to their business needs. This includes structuring the periods of performance for core IT support requirements for continuity of service with minimum transition disruptions. One method of accomplishing this objective is to establish extended periods of performance that have longer overlaps between contracts. The performance periods might be structured to allow FTC cases and matters to start and end using the same product set (i.e., aligning contract periods of performance with FTC case schedules). Data transitions, if any, would occur after a case has substantially closed and disruption from a product switch is at its lowest level.

h. Discussion of cost, performance and other trade-offs was omitted

FAR guidance provides for a full discussion of trade-offs in acquisitions. Trade-offs allow agencies to better tailor acquisitions to business needs and constraints (e.g., trading increased costs for increased security, reduced availability for reduced costs, and increased monitoring for reduced performance risk). Neither the eDSS nor the mobile device project Business Case Analyses had a reasonable discussion of these trade-offs.

The eDSS Business Case Analysis discussed three optional technical solutions, but did not effectively analyze the factors that would allow the FTC to identify the optimum solution. For example, the FTC was seeking a high-performing data analysis capability that would enable FTC attorneys and other staff to reliably and quickly review and analyze large volumes of data. However, the Business Case Analysis did not discuss any trade-offs that might incentivize offerors to provide such high-performing solutions. Similarly, the eDSS Business Case Analysis

did not include other supporting analyses (e.g., performance period analysis, functional requirements document, or a discussion of security safeguards that describes the security control objectives that any solution must accommodate) which might have identified other opportunities to reduce cost or improve performance through trade-offs.

As noted previously, the mobile device project was a commodity acquisition. The opportunity to make trade-offs in such acquisitions is more likely to be in configuring the instruments and supporting software. For example, the FTC implemented certificate-based security that increased security but had an associated operational cost in limiting the sites to which a user could connect and an administrative cost to establish and maintain certificates. These types of configuration trade-offs should be documented in instrument and product-specific artifacts.

i. Risk issues were not sufficiently considered

The FAR requires evaluation of all forms of risk (e.g., technical, performance, schedule, cost, and security) as part of acquisition planning. Both the eDSS and mobile device projects examined risk to a limited degree, with a focus on security risk. Neither project included a discussion of security requirements that identified risks and established security requirements baselines. The eDSS Business Case Analysis explicitly recognized a System Security Plan requirement. NIST and FTC policy require a System Security Plan for mobile devices -- typically a single plan with the mobile devices configured as a single information system.

The FTC's failure to effectively assess technical, performance, and schedule and cost risk was more important to eDSS than to the mobile device project. The devices and software acquired for the mobile device project are commodity products that are generally available from commercial catalogs using standard definitions. By contrast, the eDSS product is complex software where the purchaser must define the functionality and supporting environment. Also, eDSS functionality must address specialized capabilities required for use in manipulating and securing litigation and merger and acquisition data. The FTC's failure to effectively define, test, and monitor eDSS capabilities resulted in acquisition of a product that did not have needed functionality and reliability to address FTC user needs and could not scale to address workload changes. Consequently, FTC work is delayed and staff are seeking other alternatives and work-arounds to obtain needed support.

2. Ineffective project monitoring delayed corrective action and increased costs

The FTC Governance Boards are to serve as both planning and oversight entities. In planning, the Governance Boards ensure that IT investments tie directly to business needs and are properly scaled to project size and complexity. In project monitoring, the Governance Boards are to ensure, through ongoing oversight, that projects are moving toward successful completion and that problems encountered during project performance are promptly identified and escalated to appropriate management for prompt, corrective action.

The planning deficiencies identified in the preceding section showed that there continue to be systemic weaknesses in FTC IT project planning. The presence of the identified deficiencies in ongoing projects that were subject to multiple level review is evidence of the lack of maturity in project planning. For example, the OIG review showed that had the FTC followed its own acquisition procedures, completing the need, cost, risk, ROI, compatibility analyses and related activities identified in both Business Case Analysis and FAR guidance, the deficiencies and associated performance and cost problems that plagued the eDSS project could have been avoided.

OIG also identified issues in mitigating problems that could have significant, unintended adverse consequences. These illustrate a lack of maturity in project oversight. As described below, in both the eDSS and MDM projects, corrective actions were initiated without a full analysis of the solution ramifications:

- eDSS

eDSS experienced issues related to the functionality and capacity of the ZyLab software which is the key eDSS data analysis software. To mitigate one functional deficiency, the FTC funded changes to the ZyLab software (e.g., sequestration of data produced erroneously). To mitigate capacity-testing issues, the FTC eliminated its capability to effectively test the software. The loss of the testing capability did not have a significant impact on eDSS risk, as the test environments did not provide equivalent functionality to the eDSS production environment. An April 2016 TechStat, showed that it would not be cost effective to continue spending resources to resolve issues regarding system auditability and performance monitoring. While these changes may resolve the software problems in the short term, the FTC did not address the ownership and long-term issues related to funding changes to commercial products. For example, by funding the initial Zylab change, the FTC may be committing to funding ongoing software maintenance to ensure that the added functionality continues to function as the underlying software changes.

- Mobile Device Project

  Documentation showing that mobile device project functional requirements were aligned with business needs was not developed. For example, the requirement to support two different smart phone instruments was not supported in available documentation. Supporting two different instruments resulted in increased costs and project complexity that may not be justified. The FTC was moving from a single instrument with limited capability to a smart phone; without information to the contrary, moving to a multiple smart phone environment was not supported by any identified business need.

  The FTC is now researching the two-instrument decision to determine where and how the decision was made. At this time, however, since two instruments have already been deployed, the research should focus on determining how the decision was made only to ensure that similar lapses in documenting decisions for future acquisitions are avoided. The instrument question should be rephrased to determine whether it is cost effective to

continue maintaining two instruments because any decision to move to a single instrument environment will be disruptive.

3. IT Governance Program is maturing

The OIG evaluation showed that the IT Governance Program is beginning to mature. The primary source for information collected to perform this analysis was information presented to the Governance Boards and resulting Governance Board activities. Commencing in March 2016, Meeting Minutes and other Governance Program materials show that participants are "taking ownership" and are raising security and system performance concerns. For example, the Governance Boards have had continuing discussions about the problem-plagued eDSS project and how it might be corrected; and participants have requested materials documenting the rationale for concurrently deploying two different smart phones.

In addition, the FTC revised the criteria for Governance Board review to include risk as a decision factor and instituted increased monitoring of approved projects. These significant changes in approach and business process demonstrate the Chief Information Officer's commitment to maturing Governance Board deliberations and decisions and show that the Governance Boards recognize that compromise of even a very low cost project that contains no sensitive information can result in severe damage to FTC's reputation. They also reflect a core principle of enterprise risk management, now explicitly embedded in OMB's revised Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016). They also show recognition of the critical interdependency between project planning and oversight by acknowledging that projects in execution need regular oversight by the Governance Boards to ensure their successful performance.

Recommendations to Improve IT Planning and Governance

In the three projects evaluated, the OIG identified both systemic and project-specific weaknesses and deficiencies. We discuss project-specific weaknesses and associated recommendations in the next section of the report. The following 6 recommendations will promote systemic improvements to the IT Governance Boards and their vital role in supporting the FTC missions.

To ensure that projects are properly planned and documented, the FTC should adhere to the OCIO Information Technology Acquisition Strategy for a Business Case Analysis/Acquisition Plan. Specifically, the FTC should:

1. Complete applicable Business Case Analysis (BCA) elements, including a description of security requirements and how they will be met; identifying BCA requirements that are waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements including Return on Investment (ROI) analysis, and risk assessments; and documentation for instances where a FAR requirement is waived or revised.

   The OCIO IT Acquisition Strategy (which parallels FAR requirements) provides a structure that emphasizes planning for acquisitions at the earliest opportunity. Early alignment of FAR planning activities with FTC Governance processes enhances the capability to identify requirements and develop acceptance criteria and performance measurement techniques.

   The Acquisition Strategy procedures are intended to provide planning capabilities applicable to any acquisition of goods and services by a federal agency. The FTC will need to tailor the procedures in a Business Case Analysis (BCA)/Acquisition Plan to the size, complexity, and sensitivity of a requirement. For example, a complex acquisition with significant solution variability like the eDSS requires a more robust acquisition plan that the mobile device project smart phone replacement, which relied on procurement of commercial products with little development effort. The decisions regarding tailoring of the Acquisition Plan should be included in the Business Case Analysis presented for project approval.

   In its August 2011 Report, *Acquisition Planning: Opportunities to Build Strong Foundations for Better Services Contracts*, the GAO found that omission of critical planning steps was prevalent among select federal agencies and suggested increased training and techniques, such as templates and checklists, to promote adherence to agency

planning structures.[17] The FTC could incorporate this recommendation into its Business Case Analysis process and require a written justification for eliminating critical planning requirements such as a description of security requirements, functional requirements, Return on Investment (ROI), and risk assessments.

A ROI serves to define the benefits to be obtained through an investment, both quantifiable and non-quantifiable. The benefits component of the ROI shows the rationale for proposing an investment. The cost component is used to show that the anticipated benefits are worth the investment. While it might be necessary to defer preparation of an ROI, an ROI should be completed to support the budget and investment analysis processes. Where the ROI is deferred, milestones should be established to ensure that the activity is completed.

To ensure that acquisition decisions are appropriately supported and may be independently reviewed and monitored, the FTC should improve its decision documentation at all levels of the acquisition process. Specifically, the FTC should:

2. Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs decisions (including individuals, Bureaus and Offices advocating for final decisions) and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.

   Acquisitions require decisions regarding a variety of topics such as what is to be acquired, acceptance criteria, performance and security risks, project authorizations, and contract awards. Evaluating the decision-making process requires assessing the quality of the information provided to the decision-maker at the time of the decision. The quality of the documentation provided to FTC decision-makers is not consistent and in some cases is not available. For example, the eDSS BCA (approved on November 15, 2011 and last updated on December 1, 2011) did not identify all litigation functionality then in use or required to support its user base. Thus, the eDSS product required modification, at FTC expense, to provide critical, needed functionality. Similarly, there was no supporting documentation for authorizing smart phone deployment with known deficiencies.

   Meeting minutes are the primary tool used to document Governance Board agendas, deliberations, decisions, and other significant activities. Meeting Minutes should provide an agenda of planned topics for consideration, a brief summary of the discussion with emphasis on decisions reached and supporting rationales for those decisions. Meeting minutes are also a critical item for documenting decision accountability. For example, the FTC initiated roll-out of smart phones to its staff even though a number of problems

[17] Government Accountability Office, *Opportunities to Build Strong Foundations for Better Services Contracts* (August 9, 2011), *available at* www.gao.gov/products/GAO-11-672.

identified in the pilot test remained unresolved. Meeting minutes did not identify the individual or organization that authorized the smart phone acquisition and roll-out.

Meeting minutes are now beginning to capture key items that can serve as "triggers" for future Government Board action. For example, the IT Business Council Meeting Minutes in January 2016 included a discussion of a TechStat goal to determine whether the FTC should support one or two phone instruments. The decision to adopt a two-phone approach was included as a functional requirement in the mobile device project BCA approved in May 2014. The decision to deploy two types of smart phones increased deployment cost and performance risk. This is shown by the activities described in the project plan (e.g., development and testing of two different instruments, training staff to support two types of instruments, and a different risk profile for each device type). However, the data contained in the BCA was insufficient to determine the magnitude of the increase). The documentation also did not show a business need for a two-phone solution.

While Governance Board meeting minutes are improving, there still needs to be a consistent balance between level of detail to support decision accountability and document brevity. For example, the FTC often uses meeting minutes to document decisions. In such cases, meeting minutes should summarize the subject and rationale for the decisions. Without such information, the Governance Boards cannot conduct effective project oversight. Inadequate meeting minutes also cannot support auditability required by NIST and financial management guidelines.

To improve documentation consistency, facilitate project monitoring, and support project and investment accountability, the FTC should institute standard governance procedures that emphasize process repeatability, risk-based decisions, and problem escalation. Specifically, the FTC should:

3. Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.

   Two FTC documents currently form the basis for FTC IT Governance: the Program Charter and the Acquisition Strategy. These documents form a good foundation, but they need to be supported by procedures that impose a process discipline and consistency (e.g., using the language of the CIGIE maturity model, "processes need to be defined and consistently applied").[18] For example, governance procedures should include an

[18] See also National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.0 (February 12, 2014).

escalation process that describes the types of problems that must be escalated and when they must be escalated for evaluation and resolution by the Governance Boards; and how topics that are not associated with a specific project or funding request are presented for Governance Board consideration (e.g., a proposal to eliminate support for non-FTC remote devices or questions about the rationale for concurrent deployment of two different smart phones).

The FTC drafted FTC IT Governance Board Administration Work Instructions and FTC IT Business Council (ITBC) Administration Work Instructions to provide structure to the IT governance process. However, these documents were overly complex and established decision-points without assigning a decision-maker. Further, the decision-points are written with an implicit objective of limiting information presented for Board consideration and did not address escalation criteria or the need for an escalation process. The Work Instructions were not finalized. Thus, the governance process continues to function without the standard operating procedures needed to ensure process consistency and completeness. The lack of process consistency increases the level of effort required to properly document items for Board consideration and increases the risk of an inappropriate or imprudent decision.

The Governance Board should implement procedures that document its workflow. The objective should be to direct and control the workflow, not to limit items presented for consideration. It is especially useful to obtain Governance Board direction as a project or investment request is developed because it can provide input about business needs throughout the FTC as well as technical direction about organizational priorities and new technologies. For example, the Governance Program currently uses Full and Executive BCA Templates, but these documents and their use is not formally documented.

To improve the quality and consistency of project deliverables, reduce project costs, and improve the reliability of project budgets, the FTC should provide guidance in best practices for developing and documenting workload and cost estimates. Specifically, the FTC should:

4. Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.

   Effective IT acquisitions depend upon information that describes both the anticipated workload and anticipated cost. These descriptions use estimates derived from a variety of sources such as prior experience, market analysis, or modeling and simulation. Estimated workloads and costs need to follow consistent development procedures if they are to support the acquisition process (e.g., ROI analysis, should-cost estimates, and storage and computer processing requirements). The FTC does not have policy or procedural guidance for developing reliable resource or cost estimates for use in IT acquisition

planning. Current FTC estimates, such as for the eDSS, are typically rough order of magnitude (ROM) estimates or have associated constraints (e.g., cash flow estimates versus cost estimates) that are not appropriate (e.g. omission of critical items such as FTC support staff requirements).[19]

The FTC should provide guidance for developing and supporting estimates used in IT acquisitions.[20] This guidance might include criteria for the use of a ROM, acceptability for full or abbreviated system life costs, and guidance for supporting estimates (e.g., a Basis of Estimate that explains how estimates were derived). This information will improve the competitive environment by reducing error from faulty estimates and increase the likelihood that the FTC will acquire the goods and services it needs at the cost it has budgeted and expects.

To improve risk evaluation, risk management, and resource allocation, the FTC should establish organizational priorities for Information Technology and security, and associated risk thresholds. Specifically, the FTC should:

5. Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.

   A key function of the Governance Boards is to establish IT project priorities based on business needs. The Governance Boards had been discussing an approach to prioritize projects, but this approach focused on evaluating project requests. The process would rank proposed projects based on perceived value and estimated costs. While comparing proposed projects to allocate funding is a needed capability, it does not provide guidance to staff as to FTC requirements.

   The FTC should establish a prioritized list of organizational business needs that will help focus development of projects to address those needs -- i.e., identify business areas where IT investments are required to modernize existing capabilities or implement new technological approaches.

[19] Rough Order of Magnitude (ROM) - Developed when a quick estimate is needed and few details are available. Usually based on historical ratio information, it is typically developed to support what-if analyses and can be developed for a particular phase or portion of an estimate to the entire cost estimate, depending on available data. It is helpful for examining differences in high-level alternatives to see which are the most feasible. Because it is developed from limited data and in a short time, a rough order of magnitude analysis should never be considered a budget-quality cost estimate. Government Accountability Office Report GAO-09-3SP, *Cost Estimating and Assessment Guide Best Practices for Developing and Managing Capital Program Costs* (March 2009).

[20] The FTC's Business Case Analysis template provides the following regarding estimates: *describe sources of cost and non-cost data for the alternatives, level of confidence in the data and any recommendations to address insufficiency of data or low level of confidence.*

Related to the list of organizational priorities would be a risk tolerance threshold. A risk tolerance threshold describes the type and level of risk FTC is willing to accept. For example, the FTC rates reputational risk as unacceptable. The FTC receives much of the information it needs to complete its missions is through submissions by consumers and private sector entities. Should the FTC be unable to demonstrate that it can protect sensitive information, there is a high likelihood that mission performance will be degraded or costs increased. Risk thresholds will filter project proposals early in the development process by eliminating proposals where the security risk is higher than acceptable.[21]

To minimize the cost and disruption resulting from an underperforming project, the FTC should institute an escalation process that includes criteria for escalating to problems to the appropriate level for timely and effective resolution. Specifically, the FTC should:

6. Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skills and skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.

   The Governance Boards collect significant information about project performance. The Boards need a defined process that includes guidance for escalation (e.g., repetitive acceptance test failures, cost overruns). Those items escalated due to information or privacy concerns should be considered for addition to the FTC Plan of Action and Milestones (POA&M) process established under FISMA.

[21] OMB is establishing a risk-based culture for federal decision-making. This is seen in the risk requirements in the revisions to OMB Circulars A-123 and A-130. In current efforts to address OMB's revised Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* the FTC is proceeding to implement an ERM Guide, which includes development of a risk register, risk thresholds, and related assessments for its Bureaus and Offices, including the OCIO.

OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016) contains similar requirements for risk-based decisions. The long-term relationship between Circulars A-123 and A-130 has been recognized by OMB and presents an opportunity to establish an integrated risk management/internal control capability consistent across FTC that addresses both A-123 and A-130 requirements. Implementation of this OIG recommendation can be integrated into these agency-wide efforts and timetables.

Project-Specific IT Governance Deficiencies

In the first part of this report, we focused on opportunities to address weaknesses in FTC IT governance practices. The FTC is an independent federal agency with a unique dual mission to protect consumers and promote competition. Effective and reliable IT is crucial to the FTC's ability to satisfy these missions. IT governance consists of the leadership, structures, and processes that enable the FTC to make decisions to ensure that its information systems sustain and extend its strategies to complete its dual missions. In conducting our evaluation, we assessed the FTC's IT governance program through review of in-place policies and practices for maintaining and evolving FTC's and associated practices for monitoring the effectiveness of the governance program.

As stated in congressional, OMB, and GAO reports, weak IT governance programs result in information systems that do not meet organizational needs and have higher acquisition and operations and maintenance costs. In response, Congress enacted laws such as FISMA, Clinger–Cohen Act, and Federal Information Technology Acquisition Reform Act (FITARA) to require agencies to implement and follow best practices for acquisition and management of Federal information technology assets. What we found in this assessment and our FY 2015 FISMA evaluation is that the FTC governance program has appropriate policies and procedures in place, but their application is inconsistent and program monitoring is weak.

The weakness of FTC IT governance practices is evidenced by the results of our assessment of two IT projects in process (eDSS and mobile device project) and one potential project (implementation of new CUI practices) discussed in this second part of our report. The OIG selected these projects because they were identified as potential problems in our FY 2015 FISMA evaluation and have a significant impact on FTC's ability to complete its missions and protect its information assets. As shown in the succeeding discussions:

- The eDSS and mobile device projects did not deliver the anticipated functionality; eDSS is a failed project where requirements were not well defined, anticipated performance benefits were not achieved, and correction of identified deficiencies is not cost effective; and the mobile device project resulted in service delays and increased transition costs.

- The CUI effort is not yet reflected in IT system planning, increasing the potential that the FTC will not be able to cost effectively comply with program requirements, and information assets will be subject to higher security risk. For example, federal guidance is already in place to address concerns associated with the placement of CUI data at contractor facilities. This guidance is not yet included in FTC planning.

1. Efforts to Replace FTC eDSS Litigation Support System

The FTC is critically dependent on its capability to collect and analyze large volumes of digital information. The FTC initiated the eDSS project to replace its legacy data analysis capabilities with a product that provides expanded functionality, capacity, and reliability. After four years

of a five-year contract, the eDSS software has still not delivered anticipated functionality, it has demonstrated reliability problems, and users are looking for and using alternatives to complete their analyses.

a. Why this project was selected for evaluation

The FTC has approximately 1,400 staff and contractors, and 200 interns.[22] Staff activities involve the production and review of significant amounts of electronic data in support of FTC litigation activities. This process is typically referenced as e-Discovery and is bundled into the FTC e-Discovery Support System (eDSS).[23] Most information provided to the FTC comes in digital form. E-Discovery tools and techniques provide the work platform for FTC review of electronic information in litigation. Availability of reliable eDSS capabilities is thus crucial to successful execution of the FTC's dual missions.

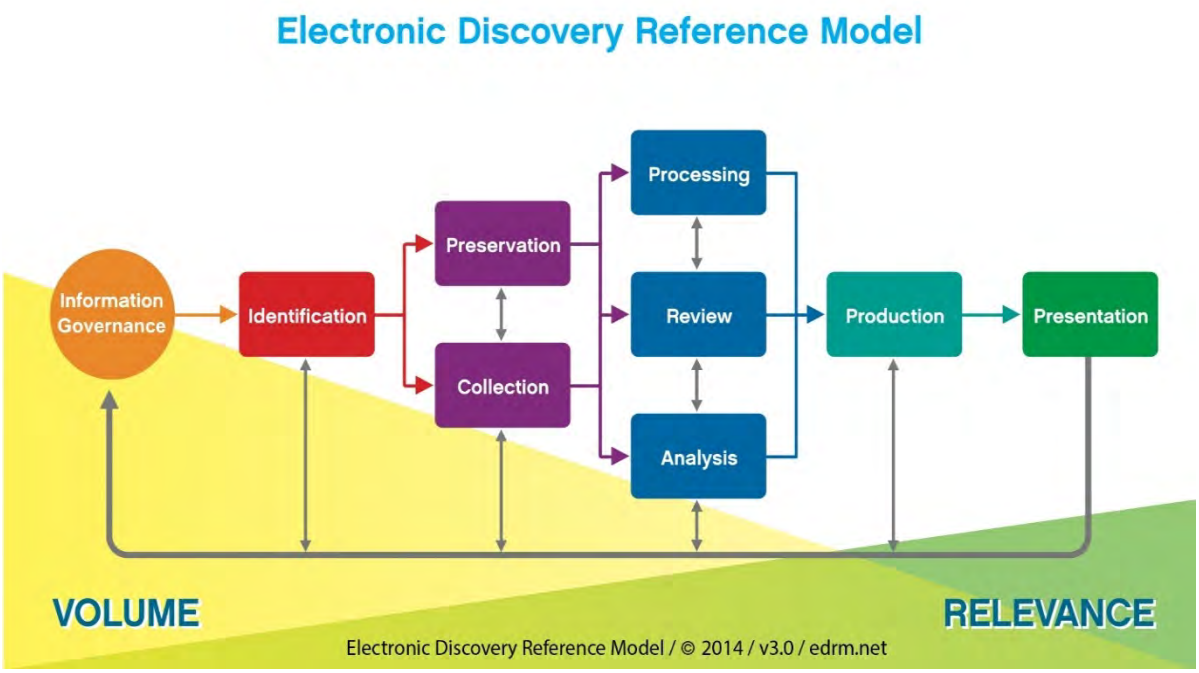
In 2005, a coalition of consumers and providers developed the Electronic Discovery Reference Model (EDRM) to address the lack of e-Discovery standards and guidelines for defining and evaluating the effectiveness of e-Discovery tools and practices. The EDRM, shown in Figure 1, is a framework that outlines standards for records management and for the recovery, discovery, and analysis of digital data. The FTC uses the EDRM in planning its data discovery and litigation support efforts. Those phases of the EDRM dealing with the discovery process are contained in the eDSS project (see Figure 2). The information governance and records management components are addressed by the FTC outside the eDSS.[24]

As described in the eDSS Business Case Analysis (approved in November 2011), the FTC provided EDRM discovery capabilities through a discrete set tools, each of which addresses a portion of needed e-Discovery capabilities. These tools are listed below and are shown in Figure 3 relative to their e-Discovery support area.

- Concordance: Litigation support
- Encase: forensic collection and analysis
- Forensic Toolkit (FTK): forensic collection and analysis
- Kazeon: forensic collection, indexing and analysis
- LexisNexis LAW Pre-Discovery: processing and production
- LexisNexis CaseSoft Suite: collaborative activities; transcript management
- Trident Preview: native document file-viewing, review

[22] Federal Trade Commission, *Statement of Objectives, Electronic Discovery Support System* (February 17, 2012).
[23] Electronic discovery (sometimes known as e-discovery, ediscovery, eDiscovery, or e-Discovery) is the electronic means of identifying, collecting and producing electronically stored information (ESI) in response to a request for production in a law suit or investigation. ESI includes, but is not limited to, emails, documents, presentations, databases, voicemail, audio and video files, social media, and web sites. See http://cdslegal.com.
[24] Electronic Discovery Reference Model (EDRM) - http://www.edrm.net and OCIO Business Case Analysis for e-Discovery Support System (December 1, 2011).

Figure 1: Electronic Discovery Reference Model



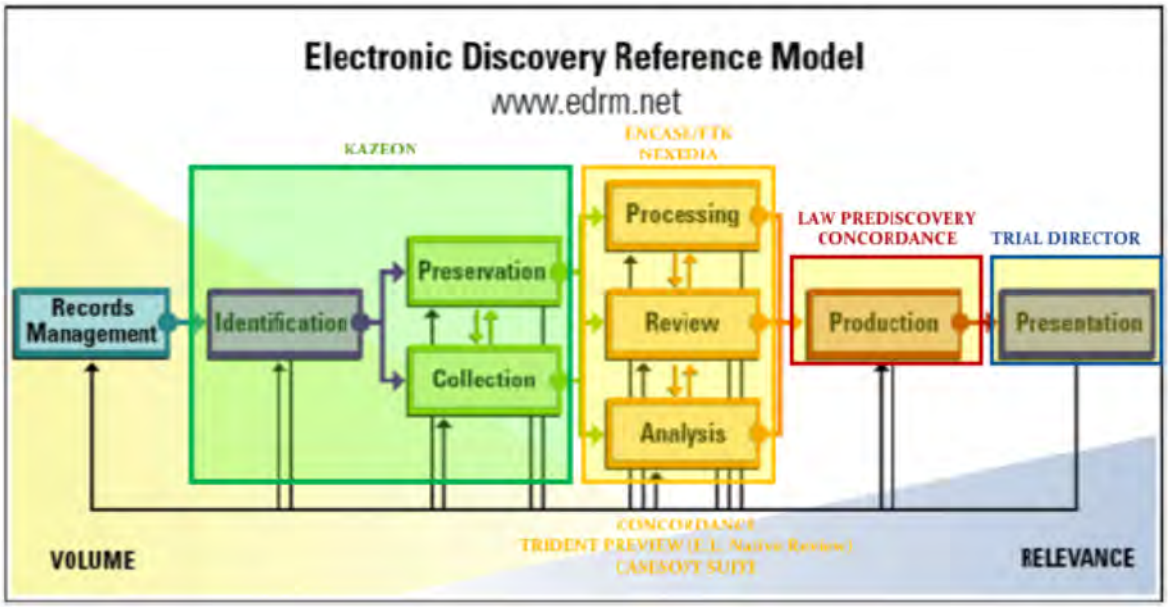
As shown in Figure 2, in 2011, the FTC assessed that its litigation support software suite could no longer meet its needs. In response, it developed a Business Case Analysis for the eDSS replacement effort. The CIO approved the plan on November 15, 2011. Even though the Business Case Analysis was incomplete and stated that cost estimates had significant variability, the Business Case Analysis approval contained no requirements or milestones for updating and review as the eDSS project proceeded and available information improved. Similarly, the approval also did not establish "stage gates" or other controls that established checkpoints to ensure the project was continuing as planned.

Figure 2: FTC Determines that its e-DSS capabilities are deficient

> [T]he FTC has seen a significant increase in the amount and types of data that is collected and reviewed and has been unable to meet the FTC's litigation needs to effectively and efficiently review and process the data collected with the current software applications. This is especially evident within the FTC's eight regional offices where users experience unacceptable system latency problems causing the current system to be ineffectual." -- eDSS Business Case Analysis, e-Discovery Support System (12/1/2011)

In its FY 2015 FISMA review, the OIG identified the eDSS as a problem project: 5-year project costs had risen from the Business Case Analysis estimate of $4.4 million - $6.1 million, to $6.45 million at contract award, with an estimated cost to completion of $7.9 million; meeting minutes, TechStats, and other Governance Board information show that the project was substantially behind schedule and underperforming; the FTC had shifted resources from test to production as the Development and Acceptance Test environments. The change was made because the Development and Test environments were not accurate representations of the Production environment and therefore provided limited test benefit and could not replicate the Production environment capacity and thus were of limited use in analyzing the eDSS workload and products scalability. The decision to eliminate of Development and Test environments recognized that it was not appropriate or cost effective to continue funding if their capability does not reduce risk; and FTC staff increased their reliance on legacy systems (that were scheduled for replacement) to meet their litigation needs.

Figure 3: EDRM with FTC e-Discovery Tool Overlay



b. Results of the eDSS Evaluation

Evaluation of the eDSS effort identified a number of planning deficiencies that intersected with deficient contractor management. For example, project planning deficiencies resulted in a failure to include appropriate performance monitoring criteria in the eDSS solicitation. Without performance metrics, the FTC did not have the tools necessary to hold the contractor accountable for its performance. The lack of performance metrics was complicated by a failure of the prime contractor to monitor project status and take appropriate action to resolve problems encountered by its subcontractor. These deficiencies resulted in an eDSS that did not provide needed support or sufficient information to effectively monitor contractor and software product performance. Further, attempts to resolve test environment deficiencies resulted in elimination of testing as an

effective control -- a decision that usually increases security risk by increasing the potential for unauthorized functionality to be installed into the production environment. However, elimination of the eDSS test environment in this instance was warranted because it could not simulate the eDSS production environment (i.e., it could not replicate production functionality).[25]

The OIG analysis also showed that during the ongoing lifecycle of the eDSS acquisition, the IT Governance process began to mature, including, as discussed in the first part of this report, the introduction of additional TechStats and incorporation of risk-based discussions. Yet, the eDSS project deficiencies showed that FTC does not consistently apply its IT planning and acquisition policies and procedures. The ability to use Governance Board materials (e.g., meeting minutes and TechStats) to identify project deficiencies now demonstrates the presence and value of IT Governance procedures for project monitoring, assignment of responsibility, and auditability.

1) eDSS did not follow FAR or FTC Planning and Acquisition Policy

Both the FAR and the OCIO IT Acquisition Strategy require a documented process for planning, conducting, and managing IT acquisitions. The FAR requirement identifies the Acquisition Plan as the primary management document. FTC procedures use the Business Case Analysis to identify requirements, link requirements to business needs, and define criteria for successful performance. The Business Case Analysis is augmented by other acquisition-related documents, providing an acquisition planning and monitoring approach that parallels FAR requirements. However, OIG analysis of the eDSS project showed that while appropriate policies and procedures for developing an appropriate project analysis were in place, the eDSS acquisition was not appropriately planned, documented, or executed.

As described in its Business Case Analysis, the eDSS was proposed as a multi-year effort with a rough order of magnitude (ROM) cost estimate between $1.3 million and $ 1.5 million for year 1 with a 5-year estimated cost ranging from $ 4.4 million and $ 5 million.[26] The current estimated completion cost is $7.9 million. The Business Case Analysis provided three estimated cost scenarios for a 5-year system life: using the current solution; a Software as a Service (SaaS) solution; and a standard software procurement with operations and maintenance (O&M) within the FTC Headquarters Datacenter. Figure 3 provides the Business Case Analysis Table of Contents. If all Business Case Analysis elements had been appropriately addressed, approvers would have had a comprehensive data analysis on which to base their authorization decision. Figure 4 provides the eDSS functional requirements.

---

[25] According to NIST guidance, "the results from static/dynamic testing and code analysis can provide important evidence that the information systems (including the components that compose those systems) will be more reliable and trustworthy." NIST Special Publication 800-53 r4.
Also see ITL Bulletin, *Combinatorial Testing for Cybersecurity and Reliability* (May 2016), *available at* http://csrc.nist.gov/publications/nistbul/itlbul2016_05.pdf.

[26] A Rough Order of Magnitude Estimate (ROM estimate) is an estimation of a project's level of effort and cost to complete. The main purpose of the ROM estimate is to provide decision makers with the information necessary to make a decision using information available at the time, on whether it makes sense to move forward with the project based on the estimated level of effort, in terms of completion time and cost.

Figure 4: eDSS Functional Requirements

Processing		**Preservation and Collection**
Deduplication		Litigation hold notification, reminders, tracking
DeNIST capabilities		Custodial survey and auditing
Password protected file detection		Index/import from network file locations/Exmerge
Decryption		Electronic mail collection
Filter/restrict (domain, file type, etc.)		Microsoft Exchange (2000, '03, '07, later)
Exception/ gap reporting		Lotus Notes (5-8 and later)
		Novell GroupWise (6.5, 7, 8, and later)
Review and Analysis		Outlook Express / Bloomberg Mail
Email/Electronic Documents		Collection/media history
Discussion threading		Scheduling of periodic collections
Domain filters		Systematic sampling/reporting
People Analytics		Enterprise search and collection
Near duplicate detection/comparison		On line
Find Similar		Off line
Data Analytics		Portable media
Content clustering, categorization or classification		Backup, peripheral, and optical media
Visualization/graphics		File System Support
Searching		EXT2, 3
Boolean		HFS, HFS+File systems/ FAT 12,16,32
Concept		NFTS File Systems/Virtual PC, Ghost, VMware File Formats
Subset Search		Palm OS, Reiser, UDF, FFS, JFS, File Systems
Hit Highlighting		Novell NWFS and NNS File Systems
Meta/Field Filtering		Legacy File Systems Supported
Document Review		
Batch Assignment/Review Management		**Integration**
Family Propagation Rules		Transcript management/search
TIF/PDF Rendering		Audio/video support - review, index, search
Native File Viewer		Tape and Archival Service
Concurrent Processing		
Redaction/Annotations		**Additional Features**
Production		Predictive analytics/coding
Export files in native or image format		Password cracking
Create major load files (XML, DAT, CSV, TXR, ASCII, etc.)		Reconstitution of PSTs
Ability to produce in stages (rolling productions)		Automated redactions (PII/SHI)
OCR/extracted text		Tiered sorting for production
File naming options (rename for DocID or Bates number)		
Endorsing image or PDF files		
Multiple production set/image handling		

The OIG's evaluation of the Business Case Analysis shows that it contained weaknesses that should have generated questions before project approval and should have added close oversight until the deficiencies were corrected.

The FAR requires that Acquisition Plans include a discussion of a number of items related to the acquisition, including business need, cost, requirements, and performance criteria. FTC acquisition policy incorporates the FAR requirements into a Business Case Analysis (see Figure 5, BCA Table of Contents). Thus, under FTC policy, the *Justification and Investment* section

Figure 5: BCA Table of Contents

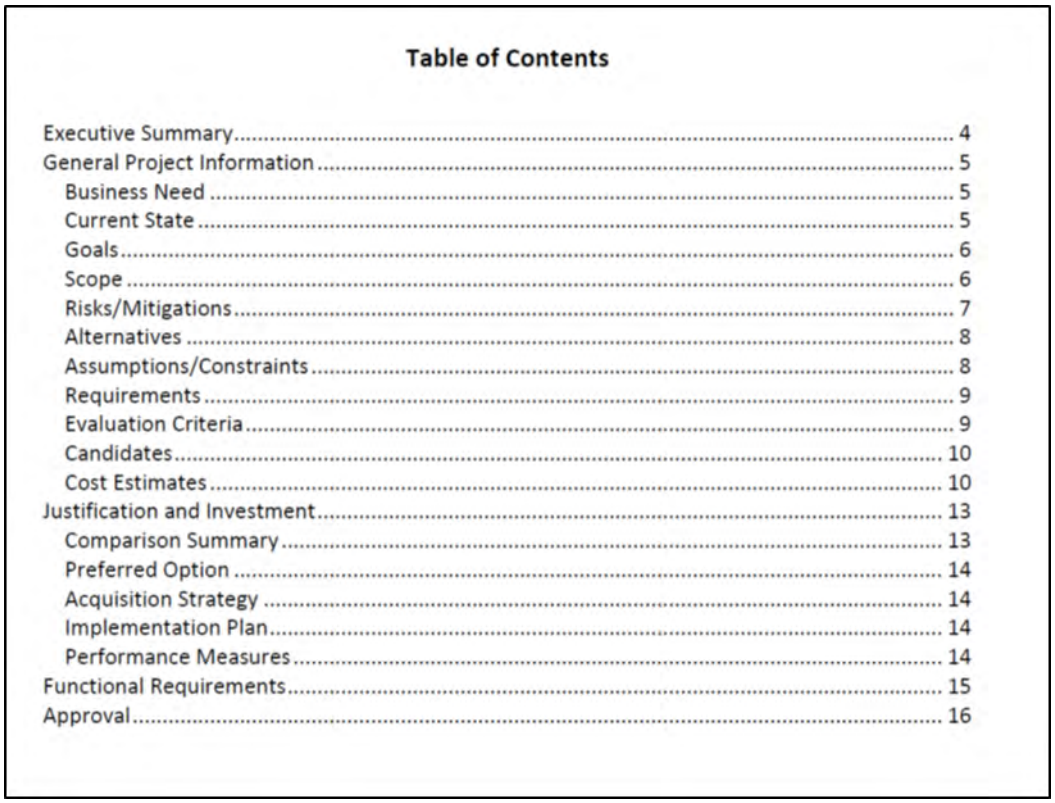


Table of Contents

provides the rationale for project and acquisition approval and identifies the resource investment required for completion. Yet, the eDSS Business Case Analysis did not provide the required supporting information.

In this review, the OIG found weaknesses in the treatment of eight key elements of the eDSS Business Case Analysis: Comparison Summary; Preferred Option; Acquisition Strategy, Implementation Plan, Performance Measures; Risks/Mitigations, and Functional Requirements:[27]

- **Comparison Summary** – The FAR and FTC policy require an Analysis of Alternatives: A description of alternative options and possible solutions, including

[27] FTC Information Technology Governance Program Charter (July 2011).

taking no action, and the risks and benefits of each option. The eDSS Comparison Summary provides the estimated costs for the eDSS project for the three alternatives considered: continue the **Current** approach; implement eDSS using a commercial shared service (**Software as a Service**); and acquire a solution and install on the FTC Headquarters Datacenter. However, Business Case Analysis comparative cost data is qualified with the following statement:

> As all of the cost data for the current system is unknown, it is unrealistic to complete a ROI calculation; however, a cash flow can be summarized for the current system and the alternatives of SaaS and software procurement.

Further, cost information provided is described as Rough Order Of Magnitude estimates. GAO cost estimating guidance states that a Rough Order of Magnitude analysis should never be considered a budget quality estimate.[28]

With this constraint, the value and reliability of the data presented are very low (a high performance risk). The FTC should have included milestones to improve information reliability and require management review as a condition for Business Case Analysis approval.

- **Preferred Option** – The Business Case Analysis proposed three pricing profiles for the eDSS technical implementation: **Current** – multiple licensed software tools acquired and installed on the FTC data center; **SaaS** – Software as a Service; and **Software Procurement** – a new licensed software product is acquired and installed on the FTC data center. Under FTC and FAR requirements, a cost analysis should provide an estimated cost and a discussion of the cost model used for each alternative considered. For the eDSS, Current should serve as a baseline/independent cost estimate since it is based on current operations and should have the highest reliability. However, the FTC characterizes eDSS current cost data as "unknown." The FTC deferred identification of an optimum solution until cost, schedule, and performance information was collected through the "Request for Proposal process." Thus, the eDSS did not include a viable cost analysis as required by the FAR and FTC policy.

- **Acquisition Strategy, Implementation Plan, Performance Measures** –These three critical topics in acquisition planning and execution were deferred until later in the RFP process. Failure to address these topic areas early in the acquisition process significantly increases performance risk. The FTC encountered significant performance shortfalls in terms of Acquisition Strategy, Implementation Plan, and Performance Measures that could have been averted or minimized if these topics had been addressed in the early stage of acquisition. For example, the Acquisition Strategy could have provided for a suite of tools to support FTC eDscovery efforts instead of a single solution, thus reducing performance risk; the Implementation could have been

[28] Government Accountability Office, *Cost Estimating and Assessment Guide, Best Practices for Developing and Managing Capital Program Costs* (March 2009).

aligned with case/project schedules to minimize transition risk and cost; and effective Performance Measures would have allowed quicker isolation of operational problems.

- **Risks/Mitigations** - The Business Case Analysis identified the eDSS project as a "significant undertaking" and identified the five major risks shown in Figure 6. Mitigations proposed for those risks were either omitted or not viable. For example, lack of a System Security Plan (SSP) and an out-of-date Privacy Impact Assessment were identified as risks, but no mitigations were provided;[29] the mitigation proposed for the Lack of Budget and Resourcing risk identified two mitigations, one of which assumed implementation of one of the alternatives being considered to minimize up front capital, and the second focused on specific, unspecified, EDRM modules. Further, the Business Case Analysis did not include a determination showing the criteria for implementing any of the proposed mitigations.

  While the Risks/Mitigations identified in the Business Case Analysis were not effectively addressed, the analysis also omitted a number of critical risk areas: cost data used to develop project cost estimates were unreliable resulting in a high risk that cost estimates will be exceeded; the lack of performance metrics increased the potential that the contractor cannot be held accountable for poor performance; the lack of reliable workload estimates meant that FTC did not have the information necessary to determine whether the eDSS could be supported on the existing FTC infrastructure; and there was no reliable data regarding the infrastructure capability to support the anticipated eDSS workload.

  The FTC also raised concerns in the Business Case Analysis about product availability necessary to address all FTC requirements, and poor quality estimates for cost and workload. However, these concerns were not recognized as performance or security risks (e.g., a multiple product solution increases the risk of delayed analyses when moving data between tools to perform a single analysis). Thus, no mitigations were proposed, and the Business Case Analysis understated performance risks.

[29] 'Information system security plan' (SSP) means a 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. OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016). An SSP may be prepared in stages where the scope and depth aligns with the nature of the system and its operational status. For example, in system planning and acquisition, security plan development focuses on system objectives and identification of security and privacy requirements (baseline requirements). Per FAR Subpart 7.1—Acquisition Plans, states that the agency head is responsible for –

> w) Ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology.

Figure 6: eDSS Risks and Mitigations

Risk	Description	Proposed Mitigation
Budget and Resourcing (Major Risk)	Funding may not be available to complete the entire end-to-end process within a single RFP/work effort.	One, focus on specific EDRM modules and develop and integrate over the system life cycle; or Two, use SaaS to minimize upfront capital expenditures to allow for the entire or at least a greater percentage of the EDRM process to be funded at one time.
Functional Requirements (Major Risk)	There may not be a singular, holistic solution that meets all functional requirements.	Apply evaluation criteria focused on the EDRM phases that impact majority of FTC litigation efforts and have the opportunity for the greatest gains in efficiency and effectiveness.
Technical Skills (Major Risk)	Needed technical support resources are not currently in-house or under contract.	Project planning will need to address additional technical support to train in-house staff or obtain these services
Process Changes (Major Risk)	Project solution results in decrease in efficiency as users are trained to use the new product and associated workflow changes.	Obtain resources for change management and business process re-engineering.
System Cutover (Major Risk)	Parallel operation is required until required initial caseload is installed and the new system is certified for operation.	Conversion will take a calendar year to execute. Resources will be included to address cutover workload.
System Security Plan	Required artifact.	No mitigation provided.
Privacy Impact Assessment	Requires updating.	No mitigation provided.

- **Functional Requirements –** As shown in Figure 4, the Business Case Analysis provided a list of functional requirements. The functional requirements demonstrate the complexity of the eDSS product. Complicating successful eDSS project performance is the lack of requirements definition. The functional requirements are listed, but their functionality is not fully defined, supported by a business need, or associated with performance criteria. Establishing functional requirements without traceability to business needs or performance criteria increases the potential that business needs will be overlooked. For example, as described more fully in the next section, the FTC determined that ZyLab had no capability to sequester information erroneously produced to FTC. Without a sequester or delete capability, ZyLab cannot be used in support of active investigations and litigation. Failure to identify the information sequestration requirement resulted in an additional cost of at least $139,724 for a custom sequestration or "clawback" solution. Until the sequestration capability was added, Zylab could not be used to support litigation efforts. Other ZyLab performance deficiencies resulted in staff using legacy systems and looking for other approaches to support their data analyses.

2) eDSS does not provide needed performance or reliability

The eDSS functional requirements listed in the Business Case Analysis (see Figure 4) focused on the functions required to conduct e-Discovery activities. The functionality needed to support administrative functions such as customer-focused performance metrics, and audit trails and logs needed to monitor system and workload operations, was not included. To address this recognized omission, the FTC stated in the eDSS Business Case Analysis that performance measures would be developed in parallel with the subsequent Request for Proposal process.

The Statement of Objectives -- the key document in the eDSS Request for Proposal process -- requires a solution providing an uptime service level of 99.5%, but does not expand on how this service level is defined or monitored. The Draft Performance Work Statement included language about a Quality Assurance Plan, but also contained the following statement regarding after contract award activities:

> the Project Manager (PM) will work with the FTC to define operational performance standards and acceptable quality levels (AQL) and define implementation milestones. The Quality Assurance Surveillance Plan (QASP) will be finalized at this time.

The eDSS After Action Report completed in August 2015 acknowledged the lack of logs, service levels, and the inability to measure and monitor performance. The only After Action Report conducted for the eDSS ZyLab product, it identified the root cause of the performance problems and provided corrective recommendations for an extended service outage. The After Action Report succinctly concluded that –

> ZyLAB infrastructure has limited or no monitoring tools available, and there is limited visibility into the ZyLAB application. The FTC had no way to measure the number of staff using ZyLAB and did not understand the affect [sic] that a spike in users would have on the two technical issues at the heart of the performance issues. This resulted in various teams struggling for weeks to figure out if the issue was our infrastructure or the application. We do not even have a basic ZyLAB troubleshooting checklist to gather information or identify issues with the application. The FTC is entirely reliant on ZyLAB Professional Services to trouble shoot the environment and we will have exhausted all available funds by mid-September.

The After Action Report also contained the following determinations about FTC capabilities to effectively manage and monitor ZyLab performance:

- There is no communications plan to report problems or outages. On a day-to day basis, problems or questions concerning ZyLAB are routed to a large number of people, separately or in groups; consequently, the Help Desk does not consistently track ZyLAB problems and questions (unlike most other applications);

- ZyLAB support is a complicated mix of overlapping contracts with poorly defined responsibilities; and

- From an infrastructure perspective, the ZyLAB environment has no redundancy. If a ZyLAB service node fails, the whole application will be down until a new server is available.

The August 2015 After Action Report listed recommendations for addressing eDSS ZyLab deficiencies that included increased funding for support services, division of responsibilities between contractor and FTC, and increased funding to develop capabilities (e.g., logging and collection of usage data). The recommendations may or may not resolve the performance problems because, as stated in the AAR, the eDSS ZyLab product and the hosting systems do not provide the information necessary to determine the performance impact of a specific change.

c. OIG Recommendations to address eDSS deficiencies

While there were a number of deficiencies that contributed to the failure of the eDSS project to deliver anticipated benefits, they all originated from a failure to develop the functional requirements that clearly defined what the investment was to accomplish, criteria for successful performance and how that performance would be monitored and measured, reliable workload estimates that could be used to determine whether the FTC data center had the capacity to support the anticipated workload, and reliable capacity data that could be used in determining whether the data center had the capacity to support the eDSS.

The root cause of the eDSS problem was failure to adhere to the OCIO IT Acquisition Strategy and FAR Acquisition Planning requirements. This does not mean that a complete Business Case Analysis or Acquisition Plan would have resulted in a successful eDSS project. It is the process and analyses used to develop the information to create the Business Case Analysis and Acquisition Plan and supporting analyses that generate the information necessary to conduct an effective solicitation that improves the potential for success.

The impact of these planning and acquisition failures was magnified by the lack of eDSS monitoring tools to identify the deficiencies; and the lack of processes to quickly escalate and resolve problems encountered projects. The eDSS acquisition should have clearly defined the required functionality; specified performance criteria and metrics for measuring successful performance; and provided an acquisition strategy that described the types of solutions that will be considered, how different solutions will be compared, and how successful performance will be defined and measured. FTC management should include a justification for its decision to waive or defer such planning requirements and establish milestones and "stage gate" requirements to ensure deferred requirements are completed.

During the course of this evaluation, the OIG identified a number of corrective actions to resolve eDSS deficiencies. These deficiencies resulted from FTC governance and acquisition issues, previously discussed, and from problems specific to the eDSS. This section provides five recommendations that the FTC should incorporate into their ongoing eDSS planning and problem resolution.

To cost effectively provide needed eDSS capabilities, the FTC should obtain a replacement contract that provides needed functionality, scalability, reliability, and availability. Specifically, the FTC should:

7. Terminate efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue support for cases in progress; prepare an After Action Report that documents the problems encountered with the current software for use as input for the acquisition of a replacement contract; and initiate a new acquisition to obtain a follow-on contract using lessons learned under the current contract to avoid similar problems.

   The current eDSS ZyLab contract was awarded in August 2012 with a 5-year period of performance and will reach the end of its performance period in August 2017. The August 2015 After Action Report proposed fixing the current contract to address performance deficiencies. Given that time horizon, the OIG assesses that the FTC should now focus its efforts on a replacement contract. The Acquisition Plan for the replacement contract should have security baselines (documented in a security plan), user-focused performance baselines, the capability to record performance metrics, and the capability to test software versions. These are all deficiencies that need resolution if a eDSS is to effectively meet FTC litigation support needs. While it may be possible to modify the current ZyLab product, this would entail a significant expenditure of FTC resources on a product advertised as a commercial, off-the-shelf solution. A more cost effective approach is to conduct a new acquisition that does not include the deficiencies inherent in the prior solicitation.

To ensure a follow-on contract provides the functionality and reliability needed to support eDSS requirements, the FTC should develop a functional requirements document that identifies and defines required functions linked to business needs and associated with acceptable performance criteria. Specifically, the FTC should:

8. Develop an eDSS functional requirements document that specifies the required capabilities (including security, privacy, and performance monitoring controls), acceptance criteria, or performance characteristics of the supplies or the performance standards for the services being acquired and state how they are related to the business need; identifies requirements for compatibility with existing or future systems or programs; describes any known cost, schedule, and capability or performance constraints; and associates requirements with acceptance criteria and performance standards.

   A fundamental acquisition requirement is an understanding of the goods and services to be acquired. The essential document memorializing this understanding is a functional requirements document, which identifies the item (e.g., software product, service, or system), relates the item to a business need, and describes criteria for successful performance. Functional performance documents are tailored to the acquisition based on scope and complexity and may have a variety of formats. The FTC should ensure that an eDSS follow-on contract has functional requirements that build on lessons learned in the current contract by clearly defining requirements, linking them to business needs, and providing measurable, user-based criteria for successful performance, along with performance testing procedures.

To ensure that all authorized functions and only authorized functions are implemented, the FTC should systematically monitor implementation of eDSS functionality and testing. Specifically, the FTC should:

9. Require maintenance of an eDSS traceability matrix that identifies authorized functions and how they have been implemented and successfully tested. The traceability matrix should be scaled to acquisition complexity, allowing required functions to be tracked from the functional requirement document, through solicitation and acceptance testing.

To ensure proper system performance, monitor ongoing customer-focused system performance, and provide a test environment that supports system troubleshooting, the FTC should maintain a comprehensive benchmarking capability. Specifically, the FTC should:

10. Maintain a set of comprehensive benchmarks that can perform acceptance testing whenever the eDSS is changed; maintain a test database that will support eDSS workload analysis and troubleshooting; use benchmark testing to establish performance baselines that can be validated throughout the eDSS contract life; and identify approaches that may be used to support stress testing analysis on a limited basis without the need to maintain a hosting facility.

    Modern information systems are complex assemblages of software, communications, and data structures. In this environment, performance testing is critical to assessing product or system accuracy, efficiency, and security. Performance should be conducted with varying workload volumes and composition to obtain an understanding of the system's capability to support the FTC workload.

    Acceptance testing validates system functionality but does not include the comprehensive testing needed to evaluate system performance under varying workload volumes and compositions. Comprehensive testing is also a useful tool to identify workload differences resulting from alternate storage techniques and in diagnosing and isolating system problems. The FTC included acceptance testing as part of its eDSS solution.

    The FTC should include benchmark testing in any follow-on eDSS contract. The testing should be used to define a benchmark that describes how the system performs during normal workloads and under varying workloads, including spikes and surges. Performance benchmarks provide valuable insights about system performance during the selection process, and as the system evolves. The benchmark tests may also be used to demonstrate how the system is likely to perform as software is "patched" or new features are added.

To minimize mission disruption and the risk of data corruption, the FTC should minimize the number and scope of system transitions. Specifically, the FTC should:

11. Align a eDSS follow-on contract period of performance to allow cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

Changes in the tools supporting eDSS can be very disruptive to FTC operations and increase work force stress by causing adverse impacts on work in progress, increasing training requirements, and requiring some level of compatibility with legacy tool sets. The FTC estimates that it takes approximately one year to convert to a new tool. With that timeline and given the difficulties and performance problems encountered with the current eDSS tool implementation, the FTC should adopt an approach where eDSS toolset changes may be accomplished with less disruption. To do so, the FTC should establish a period of performance more aligned with system life. Under this approach, transitions may be better accommodated, such as by establishing a 7-year period of performance to allow 5 years of full performance and 2 years for transition in and out or multiple contracts, thus allowing for an increased number of tools with overlapping contract periods.

2. Opportunities to improve FTC mobile device wireless services

The FTC is expanding its use of wireless devices. This expansion is driven by several factors: Mobile devices (phones, tablets, notebooks) are small physical devices with substantial information manipulation capabilities; software now provides extensive document collaboration capabilities that allows multiple individuals to concurrently review and analyze the same databases and develop documents using a single shared copy; and OMB and NARA have initiatives underway to expand information sharing and allow use of personally-owned equipment. The FTC is evolving its use of mobile devices through its Messaging Infrastructure Modernization Project to securely introduce these expanded mobile capabilities to its workforce.

a. Why this project was selected for evaluation

The FTC is critically dependent on the availability and security of its voice and data communications. The decision to replace Blackberry devices with mobile "smart phones" introduced a significant change in the risk profile as well as an opportunity to enhance the capability of the FTC workforce to complete their missions.

In May 2014 the Federal Trade Commission (FTC) Office of the Chief Information Officer (OCIO) initiated a Messaging Infrastructure Modernization Project. The objective was to provide improved email and collaboration capabilities, mobile device management, and wireless services. A key component of the initiative was to replace Blackberry telephone and e-mail service. Blackberry servers were near the end of their technological "end of life," and the future of the Blackberry and its provider, Research in Motion, was in question. Further, according to the Business Case Analysis, the OCIO viewed the replacement of the Blackberry as an opportunity to –

- Implement a system that complies with NARA/OMB requirements to manage all email in electronic format and support FTC records management and e-Discovery needs;
- Provide the FTC workforce with capabilities similar to their personal consumer experience;
- Provide a capability to edit documents, access Network Shares and the Intranet; and

- Provide faster browsing capabilities.

The May 2014 Business Case Analysis listed four assumptions for Blackberry replacement solutions:

- Provide for more than one choice of phone and operating platform;
- Provide same number of devices that are in current FTC inventory;
- Provide pool of tablets for Prototype, but can extend more as needed; and
- Provide pool of licenses for Prototype Bring Your Own Device (BYOD) program, but can include more as needed.[30]

The Blackberry replacement was incorporated into the FTC mobile device project. The project has three separate subsystems that provide wireless services, mobile devices, and configuration and management of the mobile devices. It also includes appropriate security controls to protect FTC information, monitoring of device activity, maintenance of a list of approved applications (apps), and distribution of approved applications and continuous performance optimization. In accordance with the project plan, the FTC initiated the mobile device project development effort on May 2, 2014, and was scheduled to conclude in October 2015 and transfer to an operations and maintenance (O&M) status, with an estimated cost of $1 million.[31] It also provided for two pilot tests: a Customer Pilot from September 14, 2014 through September 30, 2014, and a Technical Pilot conducted from September 17, 2014 through September 30, 2014. As of the July 20, 2015 dashboard report, the project is funded at $1.15 million with expenditures to date of $517,000 and a completion date shown as "To Be Determined (TBD)."

During its FY 2015 FISMA review, the OIG identified a number of concerns with the mobile device project:

- A complete Business Case Analysis was not prepared;
- No System Security Plan was developed for the resultant smart phone environment;
- No information was provided showing a risk-based decision to support a two instrument solution; and
- Smart phone deployment was initiated without completion of planned testing and or resolution of problems identified during testing.[32]

[30] Bring Your Own Device is an OMB initiative launched in August 2013 that encourages federal employees to use their own wireless devices (smart phones and tablets); see https://www.whitehouse.gov/digitalgov/bring-your-own-device#introduction.
[31] Minutes of the August 2014 IT Governance Board Meeting show an Original End Date and a Current End Date of 12/17/2014. The mobile device project plan showed an October 2015 end date.
[32] FTC Office of Inspector General, *Fiscal Year 2015 Federal Trade Commission Independent Evaluation of the FTC's Information Security Program and Practices*, Section 6.3, Identity and Access Management / Remote Access Management.

The OIG conducted this further review of the project to assess these concerns and determine if there continue to be governance deficiencies that result in reduced performance and increased security risk.

b. Results of the Review

The OIG review showed that the mobile device project has been hampered by the same types of deficiencies that adversely affected other FTC acquisitions for a number of years. Specifically, IT projects do not follow FTC acquisition practices in that they do not:[33]

- include required artifacts containing critical information such as functional requirements that are linked to business needs;
- associate critical functionality with criteria defining successful performance and appropriate measurement metrics;
- provide a cost/price estimate that can be used to determine the level of resources requested;
- provide a Return on Investment (ROI) or other cost/benefit analysis that provides a justification for resource requests;
- maintain decision audit trails and remedial action tracking documents; and
- contain security artifacts and risk management documentation.

These lapses in adherence to IT acquisition policy and practices had serious consequences, requiring the FTC to take extraordinary measures. These measures typically placed an increased burden on the OCIO workforce to serve as both technical managers and technical resources to resolve the problems. For example, the ITA-1 deficiencies resulted in a special OCIO initiative to mitigate the deficiencies and acquire a new infrastructure support contractor; the eDSS deficiencies resulted in poor support to the FTC workforce, unplanned expenditures of at least $139,000, with OCIO staff assuming increasing responsibilities to diagnose system problems and continued use of legacy e-Discovery tools; and the Targeted Reviews resulted in generation of unnecessary reports, where the OCIO staff served as resources for the contractor developing the reports while maintaining their own workloads. The adverse impacts of these problem acquisitions were not reflected in performance metrics because FTC metrics are not user-focused, but, instead focus on system component performance and not on service levels provided to end-users. For example, the mobile device project is comprised of two primary products: the telephone instruments, and the supporting management software. Both components require configuration of customer-focused settings to ensure they provide the functionality necessary to support FTC security and operational needs. Both the instruments and the administrative software describe the capabilities that may be enabled. The instruments in device documentation and the administrative software in its System Security Plan. The FTC policy is to develop a

[33] Contracts previously reviewed by the OIG in its FISMA reporting include: Order Number FTC-12-G-2125, eDiscovery, (8/29/2012); Contract FTC-11-H-1214, *Targeted IT Reviews and Consulting Services* (9/27/2011); and Solicitation Number FTC-09-Q-9016, *Information Technology Architecture – Infrastructure (ITA-1(September 2009)*).

System Security Plan that encompasses both the instrument and administrative software in a higher level System Security Plan that describes how the two components are configured for the FTC environment. The lack of s System Security Plan for the mobile device project increases the potential that needed controls are not in place and that the systems may not be providing the information necessary to properly manage the service.

Going forward, as the FTC adopts new, more complex technologies, the risk of a system performance failure or security breach will increase to a point where workforce-based compensating countermeasures are no longer effective. Thus, as NIST and DHS guidance and best practices illustrate, the FTC must mature its governance practices and ensure that all information systems properly install, document, and test security controls and performance metrics as part of routine IT acquisition development and maintenance practices.

1) The Business Case Analysis is incomplete

Under the FTC OCIO *Acquisition Strategy for Information Technology* and *the Messaging Modernization Project*, the mobile device project required a full Business Case Analysis. As noted previously, the purpose of a Business Case Analysis is to describe a project and provide decision-makers with the information necessary to decide whether the proposed project has a reasonable potential for success. The FTC Acquisition Strategy and OCIO 12-SA-006, *Capital Planning and Investment Control*, provide descriptions of the required content of a Business Case Analysis. The topics and level of detail are to be tailored to the size and complexity of the investment, but at a minimum, should clearly define what is requested, the anticipated benefits, criteria for success, associated risks, and anticipated cost. The FTC did not develop a formal Business Case Analysis for the mobile device project. Instead, it produced a summary contained in a *Messaging Infrastructure Modernization Project* briefing, dated May 24, 2014.

A Business Case Analysis can use different formats, but, regardless of format, it should address five critical components: what is requested, anticipated benefits, success criteria, risks, and anticipated cost. The mobile device project summary briefing did not fully address these topics. The effort consisted of a 12-page briefing dated May 2014, which showed that a significant amount of planning had been performed and that a contractor had been engaged to develop a Business Case Analysis.

The cell phone and e-mail replacement portion of the mobile device project is a project with limited variability because the instruments and the associated software are commodity items that can be acquired through the General Services Administration (GSA). The FTC has a cost baseline from its current Blackberry instrument that serves as a comparative baseline. Figure 6 shows that FTC considered three alternatives in planning its cell phone replacement. Figure 7 shows that Alternative 1 is the current state where Blackberry services is continued (estimated cost at $557 per device year; Alternative 2 is acquisition of a smart phone with partial use of shared services (estimated cost at $544 per device year), and Alternative 3 is acquisition of a smart phone with full use of shared services (estimated cost at $544 per device per year).

The summary briefing did address most of the critical Business Case Analysis topic areas at a high level. Since the mobile device project is acquiring a commodity product, the summary

briefing could suffice as a Business Case Analysis if it were accompanied with or followed by a document that provided missing detail regarding cost and security controls. For example, as shown in Figure 7, there is a cost variance between Alternatives 2 and 3. This cost variance is stated as resulting from the full use of shared services and reduced effort to integrate a mobile e-mail capability with the existing FTC e-mail capability. The missing cost elements should include a discussion of the risk associated with each alternative and a formal decision to accept the recommendation to implement Alternative 3. The missing System Security Plan should provide the controls that the FTC has elected to implement and how they are configured, tested, and monitored.

Figure 7: Mobile Device Project Cost

	FY 2014	FY2015	FY2016	FY2017	FY2018	Total
Alternative 1	$3,697,181	$2,261,057	$2,405,994	$2,212,676	$2,367,451	$12,944,358
Alternative 2	$3,421,504	$1,977,378	$2,091,261	$1,926,855	$2,080,506	$11,497,506
Alternative 3	$2,638,787	$1,635,987	$1,596,298	$1,426,854	$1,644,097	$8,942,023

Another missing item is a discussion of the functional requirements. Functional requirements should be linked to business needs. The items in Figure 8 that serve as functional requirements must be extrapolated from categories labeled as Operational Risks, Employee Needs, Future State Assumptions, and Implementation Alternatives.

Figure 8: Mobile Device Project Summary Briefing Information

Mobile Device Project Summary Briefing Analysis at May 24, 2014			
Operational Risks	• In-house email solution single point of failure • Blackberry servers are near "End of Life" • RIM/future of Blackberry is in question • Limited refresh cycle and too many hand-offs • NARA/OMB requirement to manage all email in electronic format to support records management and e-Discovery support (Dec. 31, 2016)		
Employee Needs	• FTC employees are expecting services similar to personal consumer experience • Existing carrier coverage limitations, DR needed • No formal, robust change management training program (adhoc and ineffective) • Ability to edit documents, Access Network Shares, Intranet • Access, Faster Browsing capabilities • Mailbox capacity increase requests		
Future State Assumptions	• Provide for more than one choice of phone and operating platforms • Provide same number of devices that are in current state • Provide pool of tablets for Prototype, but can extend more as needed • Provide pool of licenses for Prototype BYOD program, but can extend more as needed		
Implementation Alternatives	**FTC Data Center Improvement/Expansion** • Continue with in house device management. • Upgrade servers • Continue with Blackberry devices	**Partial Use of Shared Services** • Purchase MaaS360 • Continuous monitoring, and FISMA 2.0 compliance enforcement • Selection of Android and/or iPhone • devices with BYOD option possible • Android and/or iPad tablets	**Full Use of Shared Services** • Purchase MaaS360 • Continuous monitoring, and FISMA 2.0 compliance enforcement • Selection of Android and/or iPhone • devices with BYOD option possible • Android and/or iPad tablets
Estimated Cost	$557/Device/Year	$544/Device/Year	$544/Device/Year

2) The Summary Briefing Analysis showed the need for further research and analysis

While the summary briefing is incomplete, it still contains information demonstrating that further research and analysis was required:

- Support multiple phones and operating platforms

  Providing more than one phone and operating platform (e.g., iPhone and Android, iPad and tablets) has support, security, and cost implications. This includes maintaining multiple inventories, defining multiple sets of security controls, and training Help Desk and users in the operational characteristics of the different options. The Business Case Analysis should have identified these risks and included a discussion to justify (or

eliminate) the multiple phone approach. The justification should relate to an FTC business need. The first time the OIG saw evidence that any of these questions were asked was in the minutes of the January 14, 2016, IT Business Council meeting. At that time, the Council established as a major goal of a pending TechStat to determine whether the mobile device project going forward should be limited to a single device.

- Bring Your Own Device

  Allowing FTC staff to connect their personally-owned mobile devices to the FTC infrastructure has significant security and legal implications. The FTC currently does not allow connection of non-FTC devices to its infrastructure, other than through the SAFE2 Virtual Private Network (VPN). This policy was established to protect the infrastructure. A change in this policy should be evaluated to determine if the SAFE2 process is adequate to support increased connectivity, or if additional controls are required.

  Additionally, the FTC should evaluate whether personal devices will be able to concurrently support FTC and personal e-mail accounts. This determination may increase the potential for "leakage" of Personally Identifiable Information (PII) and will make personal information subject to FTC review. Thus, these risks warrant an executive-level decision before Bring Your Own Device implementation.

3) The mobile device project security baseline is not defined in a System Security Plan

Under the FAR, any significant information system and Business Case Analysis requires a discussion of security requirements and how they will be met (e.g., a System Security Plan (SSP)). A System Security Plan is both a planning tool and documentation artifact. For systems being planned and developed, the plan identifies the required security controls (security baseline) and how they will be addressed in the information system. As system development progresses, the plan is updated to show how controls were implemented (i.e., in place controls). Under NIST guidance, there are three types of systems: *General Support Systems* (e.g., FTC Data Center) that serve as an application host; *Major Applications* that are mission- or activity-focused and require increased control because of the data they contain (e.g., Personally Identifiable Information), their impact on the organization, and their cost; and *Minor Applications*, other than a Major Application, that requires attention to security and that security control that is typically provided by a General Support System.[34] At the FTC, the OCIO deemed the mobile device project and

[34] OMB Circular A-130, *Management of Federal Information Resources* (November 28, 2000), Appendix III, defines a "major application" as one that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application; and general support system as an interconnected set of information resources under the same direct management control that shares common functionality."
NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (April 2013) defines a minor application as "an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the *(footnote continued)*

smart phones to be Minor Applications and are thus included within the accreditation boundary of the Data Center General Support System.

Grouping the mobile device project under the FTC Data Center is appropriate because it is under the same management authority as the Data Center. Designating the mobile device project as a Minor Application is not appropriate. The Minor Application designation assumes all security and privacy controls are provided through the supporting General Support Systems – a situation that is not applicable for the mobile device project. The Minor Application designation also means that critical security artifacts that document the mobile device project were not prepared.

The OIG previously recommended that the FTC revisit its approach to designating and grouping Minor Applications, most recently in its FY 2015 FISMA evaluation. Grouping the mobile device project as a Minor Application under the Data Center has a number of negative consequences. The Data Center General Support Systems (Section 9.2.20 MaaS360 Mobile Device Management (MDM)), dated August 2014, describes the mobile device project as follows:

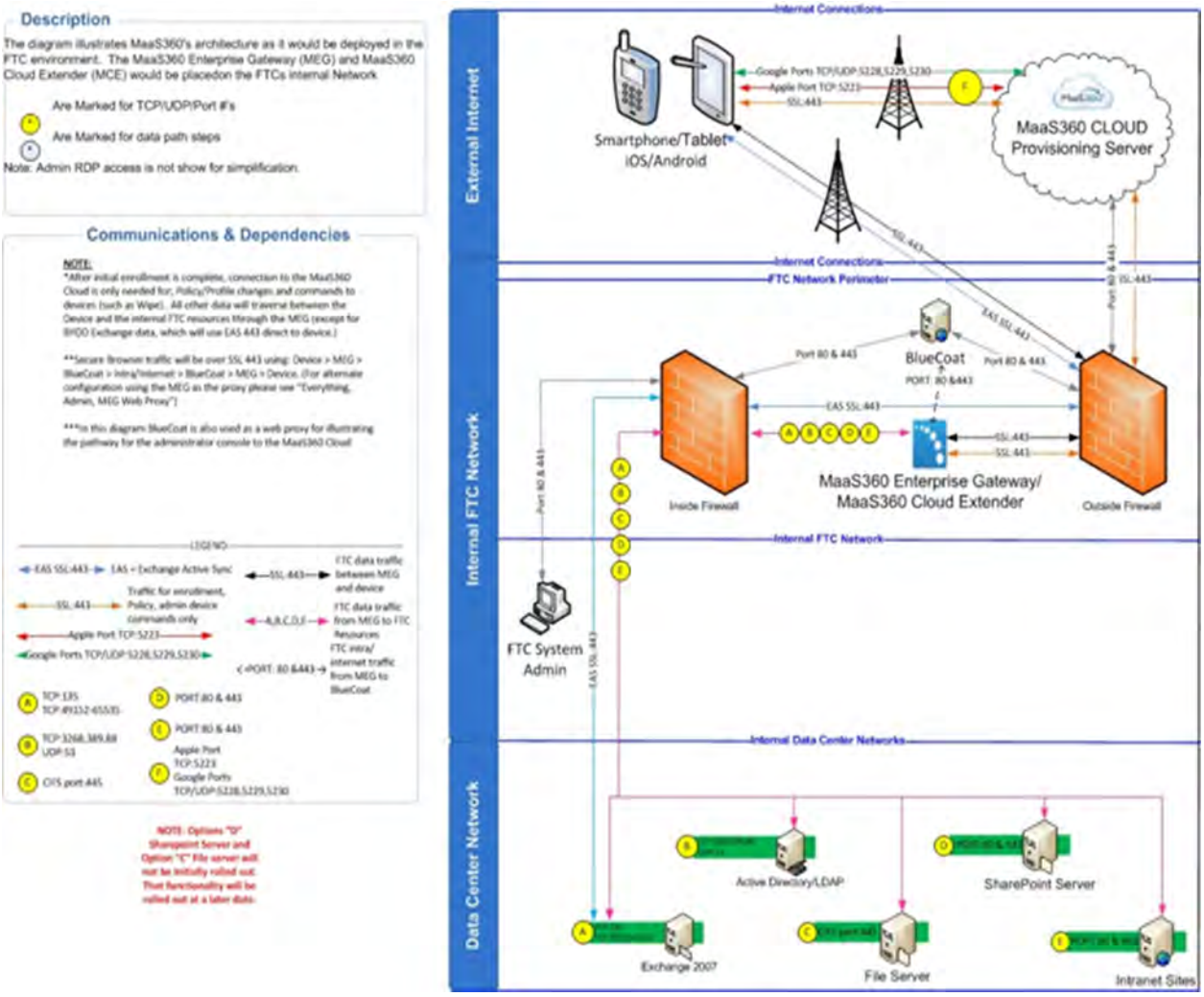
> MaaS360 MDM is a Cloud based service providing centralized management of smart phones and tablet computers belonging to the FTC. Integration to the FTC network is accomplished by two servers running the Cloud Extender and Gateway services. These servers are restricted to only be able to communicate with the IP address belonging to MaaS360. A third server will also be running Microsoft Active Sync to provide email and calendar information.

The diagram accompanying this one paragraph description (Figure 9) shows a system structure that "would be implemented," contains language regarding options that could be implemented, and does not show three servers supporting the Cloud Extender and Gateway services as stated in the text. Further, neither the diagram nor text shows the placement of this structure relative to government mandated Internet connectivity arrangements.

---

loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system."

Figure 9: MAAS6360 Implementation



Concerns with the imprecise mobile device project depiction in SSP Section 9.2.20 is compounded by the control descriptions included in Section 41 MAAS360 MOBILE DEVICE MANAGEMENT (MDM). This section presents the controls for the MaaS360 software -- control descriptions that enable the end user (i.e., FTC) to tailor security to its own environment. Thus, the controls are often stated as controls that *may be implemented* instead of describing *how* controls are implemented. Further, the control descriptions are internally inconsistent. For example, the controls describe an environment where the FTC Active Directory is used by a system that is outside the FTC security perimeter. While such an arrangement is technologically possible, the arrangement is typically more complex to ensure appropriate security control is maintained.

Treating the mobile device project as a Minor Application under the Data Center also confuses system boundaries – which may result in overlapping or omitted assignment of responsibilities. The FTC acquired MaaS360 in February 2015 under the GSA Federal Risk and Authorization

Management Program (FedRAMP). Under FedRAMP, GSA performs an analysis of each vendor's offering and issues a Provisional Authority to Operate, indicating compliance with NIST security guidance. This discrete item may be included as part of the FTC's accreditation artifacts, but FISMA and NIST guidance require that it be accompanied by a description of how the MaaS360 was configured *for the FTC* and how the supporting activities for which FTC is responsible are to be completed. A FedRAMP system would more properly be considered a "subsystem" with its own controls baseline as opposed to a Minor Application where its controls are dependent on the Data Center and there is no system-specific security baseline.

The mobile device project Privacy Impact Assessment describes the mobile device project as follows:

> The FTC Mobile Device Management (MDM) System includes three separate components that provide wireless services, mobile devices, and configuration and management of the mobile devices to include the application of security controls, monitoring device activity, the distribution of approved applications (apps), and continual performance optimization.
>
> Component 1: Mobility as a Service (MaaS) 360 is an externally hosted service used to centrally manage authorized FTC Mobile Devices and provide the following services:
>
> - Secure Mail - provides encryption, compliant with Federal Information Processing Standards (FIPS) 140-2, for secure access to FTC email, calendar, and contact tools; an official government account is created for each authorized user that is specific to their Mobile Device
> - Secure Browser - provides secure access to the FTC's intranet website and public websites
> - Mobile Application Management - provides FTC-approved enterprise apps and disables the email and calendaring functions of the Mobile Device if the user attempts to install unauthorized apps
>
> Component 2: Mobile Devices are provided by the FTC to authorized users (currently, Mobile Devices are limited to either Apple iPhone or Samsung Galaxy devices). iOS-based devices provide FIPS 140-2 hardware and data file level encryption. Samsung Android devices provide On Device Encryption (ODE) to include Secure Digital (SD) card and file-level security.
>
> Component 3: Wireless Service Provider provides talk, text, and data service for all Mobile Devices for national and international use. The Wireless Service Provider source data is not included in or authorized by any FTC information system; however, the FTC retains and analyzes monthly billing data that it receives to ensure appropriate billing rates are applied to the appropriate Mobile Devices.

This description shows that the mobile device project system boundary is different than described in the Data Center System Security Plan. The description includes the totality of the smart phone environment (e.g., installing apps, e-mail, storage of personal data), while the Data Center SSP focuses on the MaaS360. The Privacy Impact Assessment also describes special controls to protect the mobile device project environment and special rules of behavior to address the presence of personal data on an FTC system. Without reflecting these PII rules of behavior controls into the mobile device security artifacts (e.g., System Security Plan), there is a risk they will be overlooked. The PIA identifies controls that must be in place to maintain a secure environment. The PIA is a separate document where the primary target reader is non-technical, non-FTC individual. If the PIA requirement is not transferred to configuration documents with the administrators and mobile device project technical staff as the audience, there is a risk that the control will be overlooked. This may occur at initial installation or when reconfiguration is required.

4) Planning for the mobile device project development and deployment was deficient

The mobile device project included a detailed project plan that included a comprehensive list of work activities to be accomplished to select and deploy the complete project. However, the plan was overly aggressive in that it did not include slack time to accommodate unexpected events, and, critically, it did not identify project reporting and oversight as activities requiring both time and resources to complete.[35]

For example, the plan identified development of User Requirements as an activity with a duration of seven days. Collecting user requirements is also an opportunity to obtain user buy-in, techniques for monitoring user satisfaction, and information on low use but critical requirements (e.g., availability while on international travel). Collection of user requirements should also include a review phase during which the list of requirements is reviewed and approved. Experience teaches that overly aggressive scheduling provides no flexibility to accommodate unexpected delays or requirements changes. Time-constrained projects have an increased risk of experiencing delayed performance, omission of required documentation, and failure to deliver anticipated benefits. Indeed, as described in this report, the FTC encountered each of these performance, cost, and delay shortfalls in the three years since the project went on contract. A root cause of these consequences was the time-constrained project plan.

The mobile device project plan showed initiation on 5/2/2014 with a scheduled end date of 10/7/2017. As reported in an August 2014 IT Governance Board Meeting, the scheduled end date was December 17, 2014, and a July 2015 project dashboard reported the anticipated end date as "To Be Determined." Thus, as of July 2015, the mobile device project was shown as being seven months behind schedule with no definitive end date, even though the original project plan had an October 2017 end date.

[35] In Microsoft Project, Slack is the available time that a task can be delayed (or extended in Duration) without changing the project Finish date. Total Slack is not the sum of all slacks; it must be zero because on every project there is a critical path, and on the critical path, there is no slack. Because there is no slack, the Total Slack is zero.

The mobile device project plan included two pilot tests: a Technical Pilot, and a Customer Pilot. The pilots were conducted and information was collected. There was, however, no pilot test report. Thus, the findings of the tests could be expected to have limited distribution and impact.

A critical document missing from the project artifacts was a formal authorization to begin smart phone deployment. This is an especially critical document because the smart phones were deployed in advance of the original scheduled date even though reported deficiencies were not resolved. These deficiencies and others identified during deployment resulted in a delay in March 2015 to allow completion of specialized trouble shooting of the entire MaaS360 and communications infrastructure.

c. Recommendations

The mobile device project experienced a number of problems during its development and deployment. The project is now in its operations and maintenance phase. The OIG recommendations focus on correcting deficiencies that occurred during the implementation phase and will continue to adversely affect mobile device project performance and security risk.

To ensure that smart phones are appropriately documented and managed, the FTC should complete a Business Case Analysis for ongoing mobile device project operations and maintenance. Specifically, the FTC should:

12. Prepare a Business Case Analysis that provides the rationale and support for the mobile device project and its ongoing operation; include a discussion of the risks associated with the technological model deployed; and identify system functionality and relate them to business needs.

    The FTC did not complete a Business Case Analysis for the mobile device project. Instead, it used a briefing to provide some of the information that a Business Case Analysis would contain. In cases where Business Case Analyses are tailored to accommodate systems with reduced complexity and scope, FTC approvals should include a determination that Business Case Analysis requirements were adequately identified and addressed. At a minimum, requirements should be identified and related to business needs. New or unique requirements, such as support for multiple smart phones, should be subject to review of performance, risk, and cost impacts before being approved for implementation; and Requirements such as Bring Your Own Device (BYOD) that involve a material change in FTC policy should be subject to Executive review.

To ensure that the minimum controls to protect mobile devices and the information they contain and the functions they support, FTC should implement and document the implementation configuration. Specifically, the FTC should:

13. Develop a System Security Plan for the mobile device project based on NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The plan should leverage the existing Data Center ATO and Maas360 PATO as appropriate.

A System Security Plan identifies the security controls that an information system should contain and establishes a baseline for the controls a system will contain. A System Security Plan is not a "one-time" event; it provides a security baseline for an information system that is subject to change control as the system evolves and matures. The lack of a security baseline increases the potential that controls will weaken as the system evolves and software is patched because there is no authorized baseline.

The mobile device project is a complex information system consisting of physical communication devices (e.g., smart phones), a software product to manage those devices and their security configuration, and supporting policies and procedures (e.g., processes for certificate-based communications access control). The Authority To Operate (ATO) is included under the Data Center Authority to Operate. While an appropriate consolidation approach, the FTC should ensure that the mobile device project be designated as a subsystem or Major Application. The FTC should limit use of the Minor Application designation to those systems that inherit the majority, if not all, of their security controls from the information system on which it is installed. A System Security Plan should be completed for the mobile device project. If the FTC elects to continue to include the mobile device project under the Data Center General Support System, it should be defined as a subsystem to ensure security artifacts specific to project requirements are maintained.

To ensure that IT projects are completed on schedule, the FTC should develop IT project schedules that are sufficiently resilient to adjust for unanticipated delays and still complete critical activities. Specifically, the FTC should:

14. Provide training in best practices for establishing and managing project schedules; ensure project schedules contain milestones for evaluating project performance; allow slack time for resolution of unintended events; and ensure that critical tasks are completed or justification is provided if project tasks or schedules are not to be completed or are delayed.

    The FTC prepared a detailed project schedule for the smart phone deployment component of the mobile device project. However, the project encountered a number of problems as a result of planning deficiencies and management direction to bypass or change the schedule of planned activities.

    The FTC should provide training to its staff in the development and management of project schedules.[36] This training should focus on techniques to ensure that time and resource requirements are considered; milestones associated with key decision points allow performance to be evaluated against expected results and corrective action taken, if needed; and slack time allows recovery from unanticipated events. Management decisions to change schedules (e.g., elimination of pilot test reporting and an advanced deployment of smart phones) should be clearly documented to support accountability, manage associated risks, analyze lessons learned, and support auditability. Training should also stress the need to

[36] This training may be part of the training in core competencies recommended in *OIG Evaluation of the Federal Trade Commission's Office of the Chief Information Officer* (December 2015) Report No. ER 16-02.

escalate reporting on unanticipated events, performance problems, and workplace stress reflected through Help Desk reporting.

3. FTC Efforts to Protect Holdings of Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI)

In performance of its multiple missions, the FTC collects substantial volumes of information. A large volume of information is collected under the authority of specific statutes (e.g., the Hart-Scott-Rodino Antitrust Improvements Act of 1976) and in response to civil investigative demands and subpoenas. Some information is also voluntarily submitted to the FTC. The FTC's ability to collect this information is dependent on its ability to protect that information from unauthorized access, exfiltration, or tampering.

a. Why this project was selected for evaluation

The FTC conducts a multi-phased program to manage, protect, and reduce the volume of holdings of Personally Identifiable Information specifically and CUI generally. The OIG selected this program for evaluation to assess the impact of current NIST guidance and anticipated CUI requirements on the FTC's ability to effectively protect sensitive information used in performance of its missions.

The FTC's sensitive information holdings typically consist of Personally Identifiable Information, trade secrets, law enforcement, or internal decision-making data. Sensitive information may currently be labeled as Sensitive But Unclassified (SBU), For Official Use Only (FOUO), Non-Public, or Privacy Act Data.

The FTC uses a multi-phase approach to protect information entrusted to its care: information is considered "non-public" (see Rule 4.10) unless it is part of the Commission' public record (see Rule 4.9) or its release has been authorized by the Commission or the FTC Office of General Counsel (e.g., records released under the Freedom of Information Act (FOIA), see Rule 4.11). Ensuring that the agency adequately safeguards the privacy of Personally Identifiable Information (PII) is the responsibility of the Chief Privacy Officer (CPO), who reports directly to the Chairwoman. In contrast, information security, under the Federal Information Security Modernization Act (FISMA), is the responsibility of the Chief Information Officer (CIO) and is delegated to the Chief Information Security Officer (CISO). Key FTC information protection controls are: annual security and privacy training; role-based training; other FISMA information security and privacy controls; and an active program to reduce holdings of Personally Identifiable Information and other sensitive nonpublic information, emphasized by an annual Privacy Week.

In April 2013, the National Institute of Standards and Technology (NIST) consolidated federal privacy and information security controls in its Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. These NIST controls apply to CUI, regardless of type or storage medium. The CUI Program standardizes the way the Executive Branch manages information that requires safeguarding or dissemination controls under laws, regulations, or Government-wide policies, where such information does not qualify

as classified under Executive Order 13526, *Classified National Security Information* (December 29, 2009), or the Atomic Energy Act of 1954 (42 U.S.C. 2011, et seq., as amended. An Executive Branch-wide CUI policy balances the need to safeguard CUI with the public interest in sharing information appropriately and without unnecessary burden.

Federal efforts to streamline and improve the consistency of its information handling practices is a long-term, ongoing effort that gained momentum on May 7, 2008, with a White House Memorandum that established CUI as the single designator for all Sensitive But Unclassified (SBU) information in the information Sharing Environment (ISE) to facilitate the sharing of terrorism-related information. At that time, OMB designated the National Archives and Records Administration (NARA) as the Executive Agent.

On December 15, 2009, the Departments of Justice and Homeland Security released their *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information*, providing 40 recommendations for improved information handling, including a recommendation for a single, standardized framework for marking, safeguarding, and disseminating SBU information across the Federal government, eliminating the confusion resulting from other designations used to identify sensitive, unclassified information. On November 4, 2010, the President issued Executive Order (EO) 13556, *Controlled Unclassified Information*, that supported the key recommendations of the report, including the scope of CUI reform, to include all SBU information within the Executive Branch, not only terrorism-related information.

EO 13556 established a new requirement for labeling and protecting federal sensitive information that will ultimately impact all FTC information security and privacy procedures (e.g., even SBU, FOUO, non-Public, and other sensitive information labels will need to be changed to the CUI standard).

NARA maintains a website that provides a description of the CUI program and associated implementing policies and guidance (http://www.archives.gov/cui/about/). The NARA website makes it clear that the CUI program is still "a work in progress." Policies and implementing guidance is still in development and the schedule for converting to CUI labeling and marking is shown as, "To Be Determined." The site does show, however, that the CUI program will have a significant impact on current FTC practices for collecting, maintaining, and protecting federal information resources.

NARA maintains a CUI Registry that currently contains 23 information categories, a number of which have multiple subcategories. For each CUI category and subcategory, federal agencies will be expected to comply with information security requirements defined by NIST, including documents that form the basis of federal information security programs under FISMA such as:

- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*

- Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

- Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*

FTC has active information security and programs to ensure the security and integrity of its information assets. For example, within the FTC, consolidation has resulted in combining reporting and monitoring of identified security and privacy weaknesses under a single Plan of Action and Milestones (POA&M) process; and assessment of privacy controls is performed as part of the FISMA "continuous monitoring" program. Most FTC information assets are identified as CUI under existing and proposed procedures. Responding to NARA's requirement changes, once they are final, will require a significant, long-term effort to revise existing policies and procedures. In accordance with applicable law and policy, FTC information security policies will have to more strongly incorporate or be more closely coordinated with the NIST information security structure.

The FTC initiated long-term information technology planning as part of its OCIO Information Technology (IT) Governance Program. The IT Governance Program includes senior management from all FTC Bureaus and Offices. This makes the FTC OCIO Information Governance Program a critical venue for identifying and assessing the operational considerations and risks associated with the changes to FTC information handling and security policies. The OIG initiated this evaluation to determine if the IT Governance Program was fulfilling this vital planning role and was addressing the anticipated changes resulting from the CUI change and increased focus on high value databases and reducing CUI holdings.

b. Results of the CUI Evaluation

1) FTC Senior Management is aware of the CUI program but awareness has not resulted in planning requirements

The evaluation showed that FTC senior management involved with federal policy issues are generally aware of the external developments driving changes to CUI handling practices. For example, the FTC submitted comments to NARA about FTC-specific information categories that may require special safeguarding or dissemination controls, and those categories are now included in the current CUI Registry. However, meeting minutes for the Governance Boards and associated materials provided did not show that CUI had been presented as a potential requirement for inclusion in long-term planning. For example, to avoid costly and time-consuming modifications to long-term IT contracts, pending CUI changes should be a factor (even a risk factor) for contracts with a period of performance of five years or more. At the same time, because the FTC is already protecting such CUI in accordance with applicable law, rule or policy, including relevant NIST guidance, it is not clear that the final CUI rules will necessarily require modification of long-term IT contracts. Even if the CUI may impose new or special CUI marking requirements, the final CUI rules should not be expected to require dramatic shifts in information security or privacy policies and procedures affecting FTC IT contracts.

The CUI program can materially affect the manner in which FTC manages and protects its information. Currently, as noted above, the FTC categorizes all information as "non-public," unless it is on the public record under the Commission's rules (see Rule 4.9) or it is affirmatively released with either Commission or General Counsel authorization (see Rule 4.11) in response to a FOIA request or otherwise (e.g., in response to an official Congressional or GAO request, shared on a strictly confidential basis with other Government agencies for law enforcement purposes). The CUI program will require that agencies potentially adopt and follow supplemental or modified information security and privacy procedures, consistent with applicable law (e.g., FISMA, Privacy Act of 1974), rule and policy (e.g., OMB, NIST), to ensure consistent implementation and continuous monitoring of security and privacy controls. Implementation of such additional safeguards or controls, if any, may affect all aspects of information security. For example:

- Identifying, labeling, monitoring, and tracking CUI impact database designs and reporting requirements (See Figure 10 which establishes new Factors for Determining a Major Incident);

- CUI with different security requirements may impact information system designs and incident response procedures;

Figure 10: Factors for Determining a Major Incident

Factor	Definition
Sensitivity	
Classified	The confidentiality of classified information was compromised
CUI Proprietary	The confidentiality of controlled unclassified proprietary information, such as protected critical infrastructure information (PCII), controlled intellectual property, or trade secrets was compromised
CUI Privacy	The confidentiality of personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d) (7)
CUI Other	Includes all other categories of CUI not listed above
And Recoverability	
Not Recoverable	Recovery from the incident is **not possible** (e.g., sensitive data exfiltrated and posted publicly) (If information was exfiltrated, changed, deleted or otherwise compromised then incident is considered major if either 10,000 or more records or record of special importance was affected)
Not Recoverable within Specified Amount of Time	Time to recover is **unpredictable;** additional resources and outside assistance are needed (10,000 or more users affected)
Recoverable with Supplemental Resources	Time to recover **is predictable** with additional resources (If recovery takes 8 hours or more and 10,000 or more records or record of special importance are affected, then incident should be considered major)
And Mission Functional Impact	
High Functional Impact	Organization has lost the ability to provide **all** critical services to **all** system users.
Medium Functional Impact	Organization has lost the ability to provide **a** critical service to a **subset** of system users.
Or Mission Data Impact	
Exfiltration	To obtain, without authorization or in excess of authorized access, information from a system without modifying or deleting it
Modification	The act or process of changing components of information and/or systems
Deletion	To remove information from a system
Unauthorized Access	Logical or physical access without permission to a Federal agency information, system, application, or other resource
Lack of availability	When information, systems, application or services are not accessible or operational

- Metrics need to be developed to permit monitoring of CUI inventories and success of holdings reduction efforts for PII or other CUI;

- Information security requirements specifically designed for CUI (e.g., new guidelines for protection of CUI in non-federal systems) may require improved risk management;[37]

[37] National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (June 2015).

- Acquisition documents may need revision to accommodate the changed requirements as well as changes to performance criteria;

- Inventory procedures may need to be revised to include more detailed data/information inventories; and

- Procedures for controlling the volume of holdings may need to give greater consideration to digital data (digital inventories need to consider all backup versions as well as the primary database).

The OMB's October 30, 2015 request asking federal agencies to provide information about their High Value Assets (HVAs) demonstrated a need for improved inventories of digitized assets.[38] Like many federal agencies, the FTC tracks storage by devices and systems. OMB's HVA request focused on information, information characteristics, and information value. Thus, agencies, including the FTC, were estimating storage volumes and database characteristics instead of reporting using standard definitions and objective reporting metrics. As HVA reporting is now a standard reporting requirement, FTC inventories may need to be upgraded.

OMB Memorandum M-16-03, which was published on October 30, 2015, established HVAs as a standard reporting requirement, and also defined a *Major Incident* with specific reporting requirements. Shortly after the publication of M-16-03, in early November 2015, the FTC updated its Breach Notification Response Plan to incorporate all the new OMB guidance for responding to a Major Incident. The Major Incident reporting requirements implicitly defined criteria (e.g., three groupings of CUI types ("proprietary," "privacy" and "other") that cover the 23 NARA CUI Registry categories) that should be included in inventories, incident response procedures, and risk management practices to ensure FTC can properly respond in the event it experiences a Major Incident. The designation as a Major Incident is determined by the following formula:

$$\text{Major Incident} = f\big(sensitivity + recoverability + (mission\ functional\ impact\ or\ mission\ data\ impact)\big)$$

For example, The Major Incident factors would require the agency to consider the information collected through FTC mergers and acquisition activities as "CUI Proprietary," so that compromise of Hart-Scott-Rodino Act activities might constitute a Major Incident, depending upon other criteria that OMB also requires the agency to consider (i.e., recoverability, mission functional or data impact).

[38] OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (October 30, 2015).

2) FTC Governance Boards should be involved in CUI planning early in the process

Virtually all FTC mission-focused activities deal with some form of CUI. The NARA CUI program may have a significant impact on FTC system designs and operating procedures. While CUI requirements are still in the development phase, the OIG recommends that the FTC Governance Boards monitor CUI changes so their potential impact may be incorporated into FTC project planning and acquisitions.

To ensure that FTC sensitive information practices are in place and compliant with federal requirements, the FTC should include CUI program requirements as a topic for consideration in all information systems planning. Specifically, the FTC should:

15. Identify systems that may include CUI using FTC policy effective on the date a project is submitted for approval. Include control requirements of the CUI program as identified in NIST security Special Publications in FTC planning for systems, information inventories, and information protection controls. Monitor ongoing NARA and NIST CUI program activities to ensure FTC remains current with the direction and status of CUI program requirements.

    CUI requirements should be brought to the attention of IT Governance Boards so that the requirements can be included in long-term planning.

    The CUI final rules may have a significant long-term impact on FTC system designs, inventory procedures, and incident tracking and reporting. The FTC should include impact of the evolving CUI program as another decision factor that IT Governance Boards consider in their planning activities. In the short-term, this would require informing Board members of potential requirements that might impact Bureau or Office operations (e.g., changes to incident reporting requirements). In the long-term, Board participation would improve the potential that FTC will be in position to fund and implement changes for CUI handling in a timely and efficient manner.

Conclusion and Recommendations

The FTC's unique mission requires it to collect a vast amount of information from consumers, litigants, and the private sector. Due to heightened information security and privacy risks across the federal government, it must therefore pay acute attention to establishing and rapidly maturing its IT governance.

In FY 2012, the FTC sought to improve its information security and privacy programs in the face of increased threats and constrained budgets. As reported in the OIG's independent FISMA evaluations in FY 2014 and 2015, the FTC developed policies and procedures as well as updated technical governance processes to provide consistent planning and oversight of FTC IT investment and planning activities. In FY 2016, the agency did not experience a large-scale move or the turnover of key personnel as in the previous two years, and so, with the arrival of a new Chief Information Officer in July 2015, it was able to focus more on sustained planning and oversight of FTC information security investments and associated human capital and organizational issues.

Recent OIG FISMA reviews also have shown that the FTC's IT governance structure is maturing into a more efficient, risk-based information security program that will support its missions while continuing to reduce the potential of compromised systems or associated data. FTC managers and staff are now recognizing governance issues and communicating concerns to the Governance Boards. This evaluation continued to validate this salutary trend, showing that IT Governance Board members are now more proactive, are raising security and system performance concerns, and are incorporating assessments of risk and alternate solutions to technology advances and challenges.

Using documentation customarily developed as part of FTC's normal operations, we chose three projects to assess the FTC's advances to greater IT governance maturity, performing a close analysis of three projects: the e-Discovery Support System (eDSS), the mobile device Messaging Infrastructure Modernization Project, and the Controlled Unclassified Information (CUI) program. The review found that there was a failure to follow FAR Business Case Analysis/Acquisition Planning and OCIO Acquisition Strategy for Information Technology guidance that resulted in increased costs and diminished performance. It also found that ineffective project monitoring delayed corrective action and increased costs.

The FTC IT Governance Program needs to be sufficiently robust to identify and analyze the risks and benefits of various IT techniques and provide management with information necessary to weigh available options and knowledgeably select the optimum approach. Further, the decision and the supporting analysis used to identify the selected approach must be retained to maintain decision accountability and transparency, ensure timely implementation, adhere to budgeted costs, and mitigate unanticipated developments.

When implemented, the recommendations summarized below will accelerate the maturity of the FTC's IT governance, leading to greater confidence in its ability to strategically transform and direct IT investments to meet present and future organizational requirements.

1. *To ensure that projects are properly planned and documented, the FTC should adhere to the OCIO Information Technology Acquisition Strategy for a Business Case Analysis/Acquisition Plan. Specifically, the FTC should:*

   Complete applicable Business Case Analysis elements, including a description of security requirements and how they will be met; functional requirements document, Return on Investment (ROI) analysis, and risk assessment; and document instances where a BCA requirement is waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements.

2. *To ensure that acquisition decisions are appropriately supported and may be independently reviewed and monitored, the FTC should improve its decision documentation at all levels of the acquisition process. Specifically, the FTC should:*

   Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.

3. *To improve documentation consistency, facilitate project monitoring, and support project and investment accountability, the FTC should institute standard governance procedures that emphasize process repeatability, risk-based decisions, and problem escalation. Specifically, FTC should:*

   Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.

4. *To improve the quality and consistency of project deliverables, reduce project costs, and improve the reliability of project budgets, the FTC should provide guidance in best practices for developing and documenting workload and cost estimates. Specifically, the FTC should:*

   Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.

5. *To improve risk evaluation, risk management, and resource allocation, the FTC should establish organizational priorities for Information Technology and security, and associated risk thresholds. Specifically, the FTC should:*

   Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.

6. *To minimize the cost and disruption resulting from an underperforming project, the FTC should institute an escalation process that includes criteria for escalating problems to the appropriate level for timely and effective resolution. Specifically, the FTC should:*

   Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skills and skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.

7. *To cost effectively provide needed eDSS capabilities, the FTC should obtain a replacement contract that provides needed functionality, scalability, reliability, and availability. Specifically, the FTC should:*

   Terminate efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue support for cases in progress; prepare an After Action Report that documents the problems encountered with the current software for use as input for the acquisition of a replacement contract; and initiate a new acquisition to obtain a follow-on contract using lessons learned under the current contract to avoid similar problems.

8. *To ensure a follow-on contract provides the functionality and reliability needed to support eDSS requirements, the FTC should develop a functional requirements document that identifies and defines required functions linked to business needs and associated with acceptable performance criteria. Specifically, the FTC should:*

   Develop an eDSS functional requirements document that specifies the required capabilities (including security, privacy, and performance monitoring controls), acceptance criteria, or performance characteristics of the supplies or the performance standards for the services being acquired and state how they are related to the business

need; identifies requirements for compatibility with existing or future systems or programs; describes any known cost, schedule, and capability or performance constraints; and associates requirements with acceptance criteria and performance standards.

9. *To ensure that all authorized functions and only authorized functions are implemented, the FTC should systematically monitor implementation of eDSS functionality and testing. Specifically, the FTC should:*

   Require maintenance of an eDSS traceability matrix that identifies authorized functions and how they have been implemented and successfully tested. The traceability matrix should be scaled to acquisition complexity, allowing required functions to be tracked from the functional requirement document, through solicitation and acceptance testing.

10. *To ensure proper system performance, monitor ongoing customer-focused system performance, and provide a test environment that supports system troubleshooting, the FTC should maintain a comprehensive benchmarking capability. Specifically, the FTC should:*

    Maintain a set of comprehensive benchmarks that can perform acceptance testing whenever the eDSS is changed; maintain a test database that will support eDSS workload analysis and troubleshooting; and use benchmark testing to establish performance baselines that can be validated throughout the eDSS contract life. Identify approaches that may be used to support stress testing analysis on a limited basis without the need to maintain a hosting facility.

11. *To minimize mission disruption and the risk of data corruption, the FTC should minimize the number and scope of system transitions. Specifically, the FTC should:*

    Align a eDSS follow-on contract period of performance to allow cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

12. *To ensure that smart phones are appropriately documented and managed, the FTC should complete a Business Case Analysis for ongoing mobile device project operations and maintenance. Specifically, the FTC should:*

    Prepare a Business Case Analysis that provides the rationale and support for the mobile device project and its ongoing operation; include a discussion of the risks associated with the technological model deployed; and identify system functionality and relate them to business needs.

13. *To ensure that the minimum controls to protect mobile devices and the information they contain and the functions they support, the FTC should implement and document the implementation configuration. Specifically, the FTC should:*

    Develop a System Security Plan for the mobile device project based on NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The plan should leverage the existing Data Center ATO and Maas360 PATO as appropriate.

14. *To ensure that IT projects are completed on schedule, the FTC should develop IT project schedules that are sufficiently resilient to adjust for unanticipated delays and still complete critical activities. Specifically, the FTC should:*

    Provide training in best practices for establishing and managing project schedules; ensure project schedules contain milestones for evaluating project performance; allow slack time for resolution of unintended events; and ensure that critical tasks are completed or justification is provided if project tasks or schedules are not to be completed or are delayed.

15. *To ensure that FTC sensitive information practices are in place and compliant with federal requirements, the FTC should include CUI program requirements as a topic for consideration in all information systems planning. Specifically, the FTC should:*

    Identify systems that may include CUI using FTC policy effective on the date a project is submitted for approval. Include control requirements of the CUI program as identified in NIST security Special Publications in FTC planning for systems, information inventories, and information safeguard controls. Monitor ongoing NARA and NIST CUI program activities to ensure FTC remains current with the direction and status of CUI program requirements.[39]

[39] The National Archives and Records Administration Final Rule on Controlled Unclassified Information was published in the Federal Register on September 14, 2016, and is effective November 14, 2016. The FTC will be required to expend significant effort to comply.

Appendix A Acronyms and Abbreviations

AP	Acquisition Plan
BCA	Business Case Analysis
BOE	Basis of Estimate
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CMM	Continuous Monitoring Management
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
eDSS	e-Discovery Support System
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Modernization Act
FTC	Federal Trade Commission
GAO	Government Accountability Office
IGCE	Independent Government Cost Estimate
ISCM	Information System Continuous Monitoring
IT	information technology
MDM	Mobile Device Management Project
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
O&M	operations and maintenance
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
ROI	Return On Investment

Appendix B Select Federal Guidance IT Governance Policy and Guidance

OMB Memoranda	
12/09/2010	25 Point Implementation Plan to Reform Federal IT Management
12/08/2009	M-10-06, Open Government Directive (December 8, 2009) Implement the principles of transparency, participation, and collaboration.
06/08/2010	M-10-19, Fiscal Year 2012 Budget Guidance (June 8, 2010) Eliminate low-priority programs and free resources necessary to continue investments in priority areas even as overall budgets are constrained.
06/25/2010	M-10-24, Performance Improvement Guidance: Management Responsibilities and Government Performance and Results (GPRA) Federal agency guidance for GPRA and other performance management activities.
06/28/2010	M-10-26, Immediate Review of Financial Systems IT Projects Federal IT projects too often cost more than they should, take longer than necessary to deploy, and deliver solutions that do not meet business needs.
06/28/2010	M-10-27, Information Technology Investment Baseline Management Policy Provides policy direction regarding development of agency IT investment baseline management policies and defines a common structure for IT investment baseline management policy with the goal of improving transparency, performance management, and effective investment oversight.
11/03/2010	M-11-02, Sharing Data While Protecting Privacy Agencies sharing data must do so in a way that fully protects individual privacy. The public have trust in the government's ability protect personally identifiable information.
04/14/2011	M-11-17, Delivering on the Accountable Government Initiative and Implementing the GPRA Modernization Act of 2010 Provides direction that leaders set clear, ambitious goals for a limited number of outcome-focused and management priorities; agencies measure, analyze, and communicate performance information to identify successful practices to spread and problematic practices to prevent or correct; and leaders frequently conduct in-depth performance reviews to drive progress on their priorities.
08/08/2011	M-11-29, Chief Information Officer Authorities CIOs must drive the investment review process for IT investments and have responsibility over the entire Agency IT portfolio. CIOs must work to ensure IT portfolio analysis is an integral part of the yearly budget process for an agency.
06/10/2015	M-15-14, Management and Oversight of Federal Information Technology Implementation guidance for the Federal Information Technology Acquisition Reform Act (FITARA) and related information technology (IT) management practices.[40]
Government Accountability Office (GAO)	
March 2004	Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity
March 2016	Best Practices and Leading Practices in Information Technology Management http://www.gao.gov/key_issues/leading_practices_information_technology_management/issue_summary
	Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996, establish a framework to help agencies more effectively manage IT through strategic planning. Advances in technology are changing the way agencies do business.

[40] Title VIII, Subtitle D of the National Defense Authorization Act (NOAA) for Fiscal Year 2015, Pub. L. No. 11 3-91. References in the text that refer to "FITARA" refer to these sections.

Appendix C FTC Business Case Templates

FTC IT Investment Executive Business Case

All DME investments will start with an Executive Business Case. If the investment meets the criteria for a major investment, the Full Business Case, will need to be completed.

Investment Name	
Point of Contact	
Bureau/Office	
Revision Date	
Revision Comments	
Description	
< A brief description of the goal and scope of the investment>	
Justification	
<Provide an executive summary on business problems/opportunities addressed by the investment, quantitative and qualitative benefits realized, and justify investment cost against benefits>	

Cost Summary						
	Prior Years	CY (20xx)	BY (20xx)	BY+1 (20xx)	BY+2 (20xx)	Total
Products/Service						
Cost						
Cost covered by base budget						
Cost above base						

Key Stakeholders	
Executive Sponsor	
Business Lead	
IT Lead	
End User Groups	*<Describe end user groups and estimated number of users in each group>*

Strategic Alignment
<Explain how the investment aligns with (contributes towards) strategic business objectives and priorities>

Criticality/Compliance
<Cite any legislative or regulatory authority or outstanding audit findings that support the investment as a necessity.>

Opportunity/Enablement
<Does the investment enable future innovation or strategic priorities? If yes, explain in detail.>

Business and End User Impact
<Describe in detail current and future state of the business function, process, and activities impacted by the investment.> *<Also describe in detail the impact on each end user group>*

Proposed Solution Description
<Describe IT software, hardware, data components and associated services to be acquired, developed and enhanced by the investment > *<Provide conceptual solution description if detailed IT solution has not been determined>* *<Include dependencies on other IT solutions in the above descriptions>*

Analysis of Alternatives
<Briefly summarize the alternatives considered and why the above proposed solution is chosen> *(Note: a minimum of two other alternatives should be considered in addition to the proposed solution)* *<Describe your analysis of alternatives and justify your choice of the proposed solution>* *(Note: factors to consider for alternative analysis may include cost and economic viability, functional and nonfunctional requirements met, positive and negative impact on operations and end users, implementation risks, COTS/GOTS/custom, cloud/shared service/on premise, etc.>* *<Last but not the least; please describe sources of cost and non-cost data for the alternatives, level of confidence in the data and any recommendations to address insufficiency of data or low level of confidence. >*
Alternative 1 Solution and Cost Summary:
Alternative 2 Solution and Cost Summary

Analysis of Privacy and Security Risks
1) Does any component of the investment store, collect, maintain or disseminate data? Yes/No a) If yes, please describe the data (e.g., How sensitive is it? Does it include personally identifiable information (PII), such as name, SSN, date of birth, address, account number, etc.? How much data will be collected, maintained, etc.?) b) Describe the impact to the agency of data exfiltration or the loss of access to the data. 2) Is the investment an update to an existing system that handles or collects PII? Yes/No If yes, describe any of the following functions of the update that apply such as: conversion of records from paper to electronic form, conversion of information from anonymous to identifiable form, significant system changes or application of new technologies, significant merging of databases, new public access to data, use of commercial sources of data, new interagency uses of data, new collection/use/disclosure of PII, or combining new types of PII. **Note:** This analysis does not take the place of a PIA or other privacy or security assessment, which may be required by federal law. For more information on PII, see the Privacy & Information Security FAQs.

Privacy and Security Risks	Mitigation

Analysis of Other Risks
<Review of other risks such as cost, schedule, scope, technology, and management.>

Risks	Mitigation

Federal Trade Commission IT Investment Full Business Case

<Investment Name>

<Owning Organization>

<Submittal Date>

Investments with costs estimated over $1M over five years or present high risk/profile to the FTC require a Full Business Case. The FBC will be presented to the IT Business Council and the Governance Board for formal approval.

Investment Name	
Point of Contact	
Bureau/Office	
Revision Date	
Revision Comments	
Description	
< A brief description of the goal and scope of investments>	
Justification	
<Provide an executive summary on business problems/opportunities addressed by the investment, quantitative and qualitative benefits realized, and justify investment cost against benefits>	

Key Stakeholders	
Executive Sponsor	
Business Lead	
IT Lead	
End User Groups	*<Describe end user groups and estimated number of users in each group>*

Strategic Alignment
<Explain how the investment aligns with (contributes towards) strategic business objectives and priorities>

Criticality/Compliance
<Cite any legislative or regulatory authority or outstanding audit findings that support the investment as a necessity.>

Opportunity/Enablement
<Does the investment enable future innovation or strategic priorities? If yes, explain in detail.>

Business and End User Impact
<Describe in detail current and future state of the business function, process, and activities impacted by the investment.> *<Also describe in detail the impact on each end user group>*

Business and End User Impact (continued)

Key Outcome Metrics – Data used to validate the performance of the investment	
Outcome	Metrics
Examples: *<Improved responses to consumers queries>*	*Examples:* *<average consumer response time increase from xxx to yyy>*
<Reduce operating costs >	*<annual system operation and maintenance cost reduced from xxx to yyy>*
<Improved efficiency in SIL process >	*<average time to ingest data from external source to SIL reduced from xxx to yyy >*
<Improved system availability >	*<System availability increase from 99.5% to 99.9%>*

Proposed Solution Description
<Describe IT software, hardware, data components and associated services to be acquired, developed and enhanced by the investment (provide conceptual solution description if detailed IT solution has not been determined)> *<Include dependencies on other IT solutions in the above descriptions>*

Proposed Solution Cost Detail						
	Prior Years	CY (20xx)	BY (20xx)	BY+1 (20xx)	BY+2 (20xx)	**Total**
Hardware Cost (Insert new line for each item)						
Software Cost (Insert new line for each item)						
Service Cost (Insert new line for each item such as planning, project mgmt, design, develop, implement, transition, security certification training, operation, maintenance, etc.)						
Total						
Cost covered by base budget						
Cost above base						

Analysis of Alternatives
Analysis
<Briefly summarize the alternatives considered and why the above proposed solution is chosen> *(Note: a minimum of two other alternatives should be considered in addition to the proposed solution)* *<Describe your analysis of alternatives and justify your choice of the proposed solution>* *(Note: factors to consider for alternative analysis may include cost and economic viability, functional and nonfunctional requirements met, positive and negative impact on operations and end users, implementation risks, COTS/GOTS/custom, cloud/shared service/on premise, etc.>* *<Last but not the least; please describe sources of cost and non-cost data for the alternatives, level of confidence in the data and any recommendations to address insufficiency of data or low level of confidence. >*

Analysis of Alternatives (Continued)
Alternative 1 Solution and Cost Details
Alternative 2 Solution and Cost Details

Major Activities Planned				
Activity Name & Description	Deliverables	Planned Start (FYnnQn)	Planned End (FYnnQn)	Planned Cost ($)

Acquisition Plan				
Contract Name	Contract Description	Contract Type	Estimated Contract Value ($)	Estimated Period of Performance

Analysis of Privacy and Security Risks
1) Does any component of the investment store, collect, maintain or disseminate data? Yes/No a) If yes, please describe the data (e.g., How sensitive is it? Does it include personally identifiable information (PII), such as name, SSN, date of birth, address, account number, etc.? How much data will be collected, maintained, etc.?) b) Describe the impact to the agency of data exfiltration or the loss of access to the data. 2) Is the investment an update to an existing system that handles or collects PII? Yes/No If yes, describe any of the following functions of the update that apply such as: conversion of records from paper to electronic form, conversion of information from anonymous to identifiable form, significant system changes or application of new technologies, significant merging of databases, new public access to data, use of commercial sources of data, new interagency uses of data, new collection/use/disclosure of PII, or combining new types of PII. **Note:** This analysis does not take the place of a PIA or other privacy or security assessment, which may be required by federal law. For more information on PII, see the Privacy & Information Security FAQs.

Privacy and Security Risks	Mitigation

Analysis of Other Risks
<Review of other risks such as cost, schedule, scope, technology, and management.>

Risks	Mitigation

Approvals		
Role	Signature	Date
Business Sponsor		
Business Lead		
IT Lead		

Appendix D Management's Response

UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

Office of the CIO
Raghav Vajjhala
Chief Information Officer

Direct Dial
202-326-2667

MEMORANDUM

DATE: September 30, 2016

Raghav V. Vajjhala

Digitally signed by Raghav V. Vajjhala
DN: c=US, o=U. S. Government, ou=FTC, cn=Raghav V. Vajjhala
Date: 2016.09.30

FROM: Raghav Vajjhala, Chief Information Officer

TO: Roslyn Mazer, Inspector General

SUBJECT: Evaluation of the Information Technology Governance Practices

The Office of the Chief Information Officer (OCIO) has reviewed the recommendations outlined in the OIG Evaluation of FTC's Information Technology Governance Practices. They support many IT governance actions initiated by me with the support of the IT Governance Board (ITGB) since my arrival at the FTC in July of 2015. These changes include:

- Updating governance processes so that all current operational spending, not just that for new projects, receives regular review by the IT Business Council and ITGB
- In addition to techstats on the services discussed in the OIG report, techstats on network performance and disaster recovery
- Vetting of an IT Strategy and Transition Plan that addresses needs for improved performance from infrastructure operations through changes in acquisitions, re-organization of the OCIO staff, and allocation of IT operating budgets towards procurement of federally secured cloud services

The above activities identified how limitations in current infrastructure operations greatly impede the ability of the FTC to adopt emerging technology such as that for smartphones and eDSS. While documentation since my arrival supports the discussions held by the ITGB and IT Business Council on the need to improve infrastructure operations, future governance documentation shall benefit from adoption of the IG's recommendations.

The FTC response takes into account efforts already undertaken and completed – as discussed above - and sets forth completion dates to ensure that the remaining recommendations are implemented. Recommendations and dates for completion will be tracked through the FTC's Enterprise Risk Management (ERM) process. As noted in the OIG Evaluation, the FTC continually evaluates and revises its technology governance practices to meet OMB guidance and OIG reviews. The agency strives to adhere to the technology governance principles most recently articulated in the July 2016 OMB Circular A-130.

Recommendation 1: *To ensure that projects are properly planned and documented, the FTC should adhere to the OCIO Information Technology Acquisition Strategy for a Business Case Analysis/Acquisition Plan. Specifically, the FTC should*:

Complete applicable Business Case Analysis elements, including a description of security requirements and how they will be met, functional requirements document, Return On Investment (ROI) analysis, and risk assessment; and document instances where a BCA requirement is waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO already requires all Business Case Analyses (BCAs) for implementation projects to receive review and approval by the Chief Privacy Officer and Chief Information Security Officer prior to submission to the ITBC and ITGB. OCIO will develop templates to ensure BCAs contain related FAR requirements, along with security and functional requirements. In cases where this information is waived or revised, the supporting documentation will outline the rationale behind the decision, along with the risk mitigations.

Expected Completion:
FY2017 Q2

Recommendation 2: *To ensure that acquisition decisions are appropriately supported and may be independently reviewed and monitored, the FTC should improve its decision documentation at all levels of the acquisition process. Specifically, the FTC should:*

Accurately and consistently, capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.

Management Response:
Responsible Official:
Raghav Vajjhala & David Robbins

Action Plan:
Management concurs with this recommendation. OCIO has already conducted reviews with ITGB and ITBC members on upcoming acquisitions to ensure those activities support the IT Strategy and Transition Plan. Materials shared with the ITGB and ITBC individual members shall be incorporated into general governance meetings to ensure availability for future independent review. While these discussions shall focus on overall approaches and content found within Acquisition Plan, decisions regarding completion and execution of the Acquisition Plan shall continue to be conducted under the oversight of the Chief Acquisition Officer and the Chief Information Officer in accordance with the FAR.

Expected Completion:
FY2017 Q1

Recommendation 3: *To improve documentation consistency, facilitate project monitoring, and support project and investment accountability, the FTC should institute standard governance procedures that emphasize process repeatability, risk-based decisions, and problem escalation. Specifically, FTC should:*
Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan: (Note: this is also included in the response to #6)
Management concurs with this recommendation. OCIO has already established a new team as part of its re-organization, Vendor and Program Management, to develop expertise in matters of IT acquisitions. This group shall establish workflows and templates that result in Acquisition Plans sufficient for review by the ITGB and ITBC. These workflows and templates shall be enforced through updates to IT policy for governance.

Expected Completion:
FY2017 Q2

Recommendation 4: *To improve the quality and consistency of project deliverables, reduce project costs, and improve the reliability of project budgets, the FTC should provide guidance in best practices for developing and documenting workload and cost estimates. Specifically, the FTC should:*

Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO has already examined spending on IT from the past 5 years of obligation data, conducted market research on federally secured cloud services, and reviewed benchmarks on IT spending for commodity IT collected by OMB and published by GSA. From this analysis, the vast majority of IT spending supports ongoing operations and not projects. Further, IT resources receive assignments in support of project and operations. To ensure there exists viable support for workload models and costs, IT estimates now include assessments of operations and project spending. OCIO is now using this historical data on all types of spending to baseline costs for development and implementation projects along with operations of current services in support of FTC's annual budget submission across the entire FTC IT portfolio. The assumptions and basis of estimate has already been shared with ITGB and ITBC for the upcoming submission. OCIO is in process of compiling these assumptions and basis of estimate into a guidance document to be published for use by all FTE staff and updated each year based on actual performance of those projects.

Expected Completion:
FY2017 Q4 – Portfolio and Project estimating guide

Recommendation 5: *To improve risk evaluation, risk management, and resource allocation, the FTC should establish organizational priorities for Information Technology and security, and associated risk thresholds. Specifically, the FTC should:*

Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO has already established a team, Risk and Policy Management, as part of its re-organization to identify and rationalize risks and issues across all IT programs in support of the ITGB and ITBC, which includes representatives from across the FTC. Both the ITGB and ITBC have reviewed draft Risk Management and Governance Charter that will establish criteria for review of all service areas and mission critical projects as applicable. These new processes consider coverage of all portfolio spending described in the response to Recommendation 4. The final plan will be presented to the ITGB for approval or final edits prior to final implementation.

Expected Completion:
FY2017 Q2

Recommendation 6: *To minimize the cost and disruption resulting from an underperforming project, the FTC should institute an escalation process that includes criteria for escalating problems to the appropriate level for timely and effective resolution. Specifically, the FTC should:*

Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO has already established a new team as part of its re-organization, Vendor and Program Management, to develop expertise in matters of IT acquisitions. This group shall establish workflows and templates that result in Acquisition Plans sufficient for review by the ITGB and ITBC. These workflows and templates shall be enforced through updates to IT policy for governance.

Expected Completion:
FY2017 Q2

Recommendation 7: *To cost effectively provide needed eDSS capabilities, the FTC should obtain a replacement contract that provides needed functionality, scalability, reliability, and availability. Specifically, the FTC should:*

Terminate efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue support for cases in progress; prepare an After Action Report that documents the problems encountered with the current software for use as input for the acquisition of a replacement contract; and initiate a new acquisition to obtain a follow-on contract using lessons learned under the current contract to avoid similar problems.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. It reflects decisions already made by the ITGB in response to the Zylab TechStat jointly made by OCIO, BCP, BE, BC, and OGC. OCIO has terminated efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue mission critical support for cases in progress. The FTC is also using other services, such as those from the DOJ, as an interim solution.

OCIO presented an after action report in the form of a Tech Stat to the Governance Board and Business Council in April 2016 that documents the problems encountered with the current software and led to the formation of working group that shall asses requirements, costs, services in support of an Acquisition Plan for a replacement contract.

Expected Completion:
FY2017 Q4

Recommendation 8: *To ensure a follow-on contract provides the functionality and reliability needed to support eDSS requirements, the FTC should develop a functional requirements document that identifies and defines required functions linked to business needs and associated with acceptable performance criteria. Specifically, the FTC should:*

Develop an eDSS functional requirements document that specifies the required capabilities (including security, privacy, and performance monitoring controls), acceptance criteria, or performance characteristics of the supplies or the performance standards for the services being acquired and state how they are related to the business need; identifies requirements for compatibility with existing or future systems or programs; describes any known cost, schedule, and capability or performance constraints; and associates requirements with acceptance criteria and performance standards.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. A functional requirements document was created with input from the user community for the procurement of the current eDSS application, Zylab. The functional requirements document for the new eDSS solution is being developed and refined as we continue to work with the stakeholders across the FTC. Once completed and approved, the requirements document will identify and define required functions linked to business needs and acceptable performance criteria. Special attention will be given to ensure that user-focused metrics that support end-user activities are included, in addition to performance metrics.

Expected Completion:
Functional Requirements v1.0 FY2017 Q2
Final Functional Requirements FY2017 Q4

Recommendation 9: *To ensure that all authorized functions and only authorized functions are implemented, the FTC should systematically monitor implementation of eDSS functionality and testing. Specifically, the FTC should:*

Require maintenance of an eDSS traceability matrix that identifies authorized functions and how they have been implemented and successfully tested. The traceability matrix should be scaled to acquisition complexity, allowing required functions to be tracked from the functional requirement document, through solicitation and acceptance testing.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO will develop and maintain an eDSS requirements traceability matrix that identifies approved functions, and how those functions are implemented and tested.

Expected Completion:
eDSS Requirements Traceability Matrix v1.0 FY2017 Q3 eDSS Requirements Traceability Matrix v1.0 (implemented and tested) FY2018 Q2

Recommendation 10: *To ensure proper system performance, monitor ongoing customer-focused system performance, and provide a test environment that supports system troubleshooting, the FTC should maintain a comprehensive benchmarking capability. Specifically, the FTC should:*

Maintain a set of comprehensive benchmarks that can perform acceptance testing whenever the eDSS is changed; maintain a test database that will support eDSS workload analysis and troubleshooting; and use benchmark testing to establish performance baselines that can be

validated throughout the eDSS contract life. Identify approaches that may be used to support stress testing analysis on a limited basis without the need to maintain a hosting facility.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. To ensure proper performance for the eDSS system, OCIO will continue to:

- develop and maintain a comprehensive set of benchmarks
- continuously monitor customer-focused system performance
- provide a test environment that supports system troubleshooting
- work to establish performance baselines that can be validated throughout the eDSS contract life.

Expected Completion:
FY2018 Q3

Recommendation 11: *To minimize mission disruption and the risk of data corruption, the FTC should minimize the number and scope of system transitions. Specifically, the FTC should:*

Align a eDSS follow-on contract period of performance to allow cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO continues to work to ensure the follow-on support and replacement efforts for eDSS will include a transition strategy that allows cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

Expected Completion:
FY2018 Q3

Recommendation 12: *To ensure that smart phones are appropriately documented and managed, the FTC should complete a Business Case Analysis for ongoing mobile device project operations and maintenance. Specifically, the FTC should:*

Prepare a Business Case Analysis that provides the rationale and support for the mobile device project and its ongoing operation; include a discussion of the risks associated with the technological model deployed; and identify system functionality and relate it to business needs.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO presented a Tech Stat for the mobile device project to the Governance Board and Business Council in February 2016. We will continue to provide updates to the Board on the mobile device project and its ongoing operation and outline new business requirements, gaps, risks, functionality and relate them to business needs.

Expected Completion:
FY2017 Q1

Recommendation 13: *To ensure that the minimum controls to protect mobile devices and the information they contain and the functions they support, the FTC should implement and document the implementation configuration. Specifically, the FTC should:*

Develop a System Security Plan for the mobile device project based on NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The plan should leverage the existing Data Center ATO and Maas360 PATO as appropriate.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO will update the existing System Security Plan for the mobile device project based on NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations, leveraging the existing Data Center ATO and Maas360 PATO as appropriate. The milestones for completion of the plan include:

- Review FedRAMP PATO for Maas360 and sign an acceptance memo
- Create the structure in CSAM documenting control inheritance,
- Document hybrid and system specific controls in CSAM, including documenting the mobile device controls for which the FTC is responsible
- Assess the newly documented controls and create POAMs in CSAM

Expected Completion:
FY2017 Q2 – System Security Plan for FTC MDM

Recommendation 14: *To ensure that IT projects are completed on schedule, the FTC should develop IT project schedules that are sufficiently resilient to adjust for unanticipated delays and still complete critical activities. Specifically, the FTC should:*

Provide training in best practices for establishing and managing project schedules; ensure project schedules contain milestones for evaluating project performance; allow slack time for resolution of unintended events; and ensure that critical tasks are completed or justification is provided if project tasks or schedules are not to be completed or are delayed.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. Through the OCIO re-organization, the CIO has already communicated to all staff the need to obtain skills in Clinger-Cohen competencies, which include program and project management. Additionally, the CIO has already authorized one telework day a month for all staff to engage in training for the competencies. Lastly, OCIO managers will offer individual training plans to each employee, which will include the recommendation to complete project management training. The individual training plans will identify the skills necessary to plan and manage projects within the FTC environment

Expected Completion:
FY2017 Q2

Recommendation 15: *To ensure that FTC sensitive information practices are in place and compliant with federal requirements, the FTC should include CUI program requirements as a topic for consideration in all information systems planning. Specifically, the FTC should:*

Identify systems that may include CUI using FTC policy effective on the date a project is submitted for approval. Include control requirements of the CUI program as identified in NIST Special Publications in FTC planning for systems, information inventories, and information protection controls. Monitor ongoing NARA and NIST CUI program activities to ensure the FTC remains current with the direction and status of CUI program requirements.

Management Response:
Responsible Official:
Raghav Vajjhala & Jeffrey Nakrin

Action Plan:
Management concurs with this recommendation. OCIO has already started the process of revising the Risk Management and Governance policy and will integrate the requirement to identify systems that may include CUI. Additionally, our FISMA inventory database will be

revised to include a CUI type indicator and our policies will be revised to assure that the control requirements of the CUI program as identified in NIST security Special Publications are taken into consideration when planning for systems and selecting information safeguard controls. The Records and Filings Office will continue to monitor NARA and NIST CUI program activities and alert agency officials of changes that affect the agency's approach to managing CUI on its systems.

Expected Completion:
CPIC Policy Revision FY2017 Q1
FISMA Inventory Database Revision FY2017 Q1
Policy Revision to incorporate CUI controls FY2017 Q2

Appendix E OIG Analysis of the FTC Response

The OIG provided a draft of this report to the FTC. The FTC's response is included in Appendix D. Below we discuss the OIG's analysis of the FTC's response and actions necessary to close the recommendations.

Recommendation 1: *To ensure that projects are properly planned and documented, the FTC should adhere to the OCIO Information Technology Acquisition Strategy for a Business Case Analysis/Acquisition Plan. Specifically, the FTC should*:

Complete applicable Business Case Analysis elements, including a description of security requirements and how they will be met, functional requirements document, Return On Investment (ROI) analysis, and risk assessment; and document instances where a BCA requirement is waived or revised, with supporting justification and risk mitigations. Ensure the BCA considers related FAR requirements.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO already requires all Business Case Analyses (BCAs) for implementation projects to receive review and approval by the Chief Privacy Officer and Chief Information Security Officer prior to submission to the ITBC and ITGB. OCIO will develop templates to ensure BCAs contain related FAR requirements, along with security and functional requirements. In cases where this information is waived or revised, the supporting documentation will outline the rationale behind the decision, along with the risk mitigations.

Expected Completion:
FY2017 Q2

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 2: *To ensure that acquisition decisions are appropriately supported and may be independently reviewed and monitored, the FTC should improve its decision documentation at all levels of the acquisition process. Specifically, the FTC should:*

Accurately and consistently capture Information Technology Governance Board planning decisions related to business needs and supporting rationales for those decisions. Information documenting Board decisions may be included in separate documentation or meeting minutes.

Management Response:
Responsible Official:
Raghav Vajjhala & David Robbins

Action Plan:
Management concurs with this recommendation. OCIO has already conducted reviews with ITGB and ITBC members on upcoming acquisitions to ensure those activities support the IT Strategy and Transition Plan. Materials shared with the ITGB and ITBC individual members shall be incorporated into general governance meetings to ensure availability for future independent review. While these discussions shall focus on overall approaches and content found within Acquisition Plan, decisions regarding completion and execution of the Acquisition Plan shall continue to be conducted under the oversight of the Chief Acquisition Officer and the Chief Information Officer in accordance with the FAR.

Expected Completion: FY2017 Q1

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 3: *To improve documentation consistency, facilitate project monitoring, and support project and investment accountability, the FTC should institute standard governance procedures that emphasize process repeatability, risk-based decisions, and problem escalation. Specifically, FTC should:*

Develop and institute standard operating procedures with associated work instructions to support acquisition proposals and decisions, including workflows, milestones, escalation criteria, and project monitoring and tracking procedures.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan: (Note: this is also included in the response to #6)
Management concurs with this recommendation. OCIO has already established a new team as part of its re-organization, Vendor and Program Management, to develop expertise in matters of IT acquisitions. This group shall establish workflows and templates that result in Acquisition Plans sufficient for review by the ITGB and ITBC. These workflows and templates shall be enforced through updates to IT policy for governance.

Expected Completion:
FY2017 Q2

OIG Analysis: The OIG believes that this action plan is adequate to address Recommendation 3 as long as the Vendor and Program Management team combines and standardizes the workflows, templates, and procedures (e.g., tracking and problem

escalation) as work instructions or standard operating procedures that facilitate documentation consistency, project improvement, and repeatability.

Recommendation 4: *To improve the quality and consistency of project deliverables, reduce project costs, and improve the reliability of project budgets, the FTC should provide guidance in best practices for developing and documenting workload and cost estimates. Specifically, the FTC should:*

Issue guidance for developing and documenting reliable cost and workload estimates used to support acquisitions. The guidance should include selection and documentation of cost and workload models, development of a basis of estimate that documents procedures used to develop the estimates, and factors affecting estimate reliability.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO has already examined spending on IT from the past 5 years of obligation data, conducted market research on federally secured cloud services, and reviewed benchmarks on IT spending for commodity IT collected by OMB and published by GSA. From this analysis, the vast majority of IT spending supports ongoing operations and not projects. Further, IT resources receive assignments in support of project and operations. To ensure there exists viable support for workload models and costs, IT estimates now include assessments of operations and project spending. OCIO is now using this historical data on all types of spending to baseline costs for development and implementation projects along with operations of current services in support of FTC's annual budget submission across the entire FTC IT portfolio. The assumptions and basis of estimate has already been shared with ITGB and ITBC for the upcoming submission. OCIO is in process of compiling these assumptions and basis of estimate into a guidance document to be published for use by all FTE staff and updated each year based on actual performance of those projects.

Expected Completion:
FY2017 Q4 – Portfolio and Project estimating guide

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 5: *To improve risk evaluation, risk management, and resource allocation, the FTC should establish organizational priorities for Information Technology and security, and associated risk thresholds. Specifically, the FTC should:*

Require the development of FTC Information Technology and security organizational priorities to guide Governance Board review and approval of projects and investments by identifying and ranking topic areas where information systems or processes need improvement to reduce costs or improve performance; establish risk thresholds by identifying the level of risk of a system failure or data breach that the FTC is willing to tolerate; and periodically review and revise organizational priorities and risk thresholds.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO has already established a team, Risk and Policy Management, as part of its re-organization to identify and rationalize risks and issues across all IT programs in support of the ITGB and ITBC which includes representatives from across the FTC. Both the ITGB and ITBC have reviewed draft Risk Management and Governance Charter that will establish criteria for review of all service areas and mission critical projects as applicable. These new processes consider coverage of all portfolio spending described in the response to Recommendation 4. The final plan will be presented to the ITGB for approval or final edits prior to final implementation.

Expected Completion:
FY2017 Q2

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 6: *To minimize the cost and disruption resulting from an underperforming project, the FTC should institute an escalation process that includes criteria for escalating problems to the appropriate level for timely and effective resolution. Specifically, the FTC should:*

Implement an escalation process that promotes, though FTC's continuous monitoring processes, identification of potential performance problems or opportunities for improvement; identifies organizations with the skills and skill levels necessary to research and resolve project issues by problem area and skill level; implements problem tracking from identification to resolution; and establishes timelines for problem resolution and for routine (e.g., weekly, monthly, quarterly) monitoring of compliance with those timelines.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO has already established a new team as part of its re-organization, Vendor and Program Management, to develop expertise in matters of IT acquisitions. This group shall establish workflows and

templates that result in Acquisition Plans sufficient for review by the ITGB and ITBC. These workflows and templates shall be enforced through updates to IT policy for governance.

Expected Completion:

FY2017 Q2

OIG Analysis: The OIG believes that this action plan is adequate to address Recommendation 6 as long as the Vendor and Program Management team combines and standardizes the workflows, templates, and procedures (e.g., tracking and problem escalation) as work instructions or standard operating procedures that facilitate documentation consistency, project improvement, and repeatability.

Recommendation 7: *To cost effectively provide needed eDSS capabilities, the FTC should obtain a replacement contract that provides needed functionality, scalability, reliability, and availability. Specifically, the FTC should:*

Terminate efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue support for cases in progress; prepare an After Action Report that documents the problems encountered with the current software for use as input for the acquisition of a replacement contract; and initiate a new acquisition to obtain a follow-on contract using lessons learned under the current contract to avoid similar problems.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. It reflects decisions already made by the ITGB in response to the Zylab TechStat jointly made by OCIO, BCP, BE, BC, and OGC. OCIO has terminated efforts to remedy deficiencies in the current eDSS product, except those actions necessary to continue mission critical support for cases in progress. The FTC is also using other services, such as those from the DOJ, as an interim solution. OCIO presented an after action report in the form of a Tech Stat to the Governance Board and Business Council in April 2016 that documents the problems encountered with the current software and led to the formation of working group that shall asses requirements, costs, services in support of an Acquisition Plan for a replacement contract.

Expected Completion:
FY2017 Q4

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 8: *To ensure a follow-on contract provides the functionality and reliability needed to support eDSS requirements, the FTC should develop a functional requirements document that identifies and defines required functions linked to business needs and associated with acceptable performance criteria. Specifically, the FTC should:*

Develop an eDSS functional requirements document that specifies the required capabilities (including security, privacy, and performance monitoring controls), acceptance criteria, or performance characteristics of the supplies or the performance standards for the services being acquired and state how they are related to the business need; identifies requirements for compatibility with existing or future systems or programs; describes any known cost, schedule, and capability or performance constraints; and associates requirements with acceptance criteria and performance standards.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. A functional requirements document was created with input from the user community for the procurement of the current eDSS application, Zylab. The functional requirements document for the new eDSS solution is being developed and refined as we continue to work with the stakeholders across the FTC. Once completed and approved, the requirements document will identify and define required functions linked to business needs and acceptable performance criteria. Special attention will be given to ensure that user-focused metrics that support end-user activities are included, in addition to performance metrics.

Expected Completion:
Functional Requirements v1.0 FY2017 Q2
Final Functional Requirements FY2017 Q4

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 9: *To ensure that all authorized functions and only authorized functions are implemented, the FTC should systematically monitor implementation of eDSS functionality and testing. Specifically, the FTC should:*

Require maintenance of an eDSS traceability matrix that identifies authorized functions and how they have been implemented and successfully tested. The traceability matrix should be scaled to acquisition complexity, allowing required functions to be tracked from the functional requirement document, through solicitation and acceptance testing.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO will develop and maintain an eDSS requirements traceability matrix that identifies approved functions, and how those functions are implemented and tested.

Expected Completion:
eDSS Requirements Traceability Matrix v1.0 FY2017 Q3
eDSS Requirements Traceability Matrix v1.0 (implemented and tested) FY2018 Q2

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 10: *To ensure proper system performance, monitor ongoing customer-focused system performance, and provide a test environment that supports system troubleshooting, the FTC should maintain a comprehensive benchmarking capability. Specifically, the FTC should:*

Maintain a set of comprehensive benchmarks that can perform acceptance testing whenever the eDSS is changed; maintain a test database that will support eDSS workload analysis and troubleshooting; and use benchmark testing to establish performance baselines that can be validated throughout the eDSS contract life. Identify approaches that may be used to support stress testing analysis on a limited basis without the need to maintain a hosting facility.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. To ensure proper performance for the eDSS system, OCIO will continue to:

- develop and maintain a comprehensive set of benchmarks
- continuously monitor customer-focused system performance
- provide a test environment that supports system troubleshooting
- work to establish performance baselines that can be validated throughout the eDSS contract life.
-

Expected Completion:
FY2018 Q3

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 11: *To minimize mission disruption and the risk of data corruption, the FTC should minimize the number and scope of system transitions. Specifically, the FTC should:*

Align a eDSS follow-on contract period of performance to allow cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO continues to work to ensure the follow-on support and replacement efforts for eDSS will include a transition strategy that allows cases/matters to proceed from initiation to completion with little or no disruption from a transfer to a new system or hosting facility.

Expected Completion:
FY2018 Q3

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 12: *To ensure that smart phones are appropriately documented and managed, the FTC should complete a Business Case Analysis for ongoing mobile device project operations and maintenance. Specifically, the FTC should:*

Prepare a Business Case Analysis that provides the rationale and support for the mobile device project and its ongoing operation; include a discussion of the risks associated with the technological model deployed; and identify system functionality and relate it to business needs.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO presented a Tech Stat for the mobile device project to the Governance Board and Business Council in February 2016. We will continue provide updates to the Board on the mobile device project and its ongoing operation and outline new business requirements, gaps, risks, functionality and relate them to business needs.

Expected Completion:
FY2017 Q1

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 13: *To ensure that the minimum controls to protect mobile devices and the information they contain and the functions they support, the FTC should implement and document the implementation configuration. Specifically, the FTC should:*

Develop a System Security Plan for the mobile device project based on NIST SP 800-53 r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The plan should leverage the existing Data Center ATO and Maas360 PATO as appropriate.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. OCIO will update the existing System Security Plan for the mobile device project based on NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations, leveraging the existing Data Center ATO and Maas360 PATO as appropriate. The milestones for completion of the plan include:

- Review FedRAMP PATO for Maas360 and sign an acceptance memo
- Create the structure in CSAM documenting control inheritance,
- Document hybrid and system specific controls in CSAM, including documenting the mobile device controls for which the FTC is responsible
- Assess the newly documented controls and create POAMs in CSAM

Expected Completion:
FY2017 Q2 – System Security Plan for FTC MDM

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 14: *To ensure that IT projects are completed on schedule, the FTC should develop IT project schedules that are sufficiently resilient to adjust for unanticipated delays and still complete critical activities. Specifically, the FTC should:*

Provide training in best practices for establishing and managing project schedules; ensure project schedules contain milestones for evaluating project performance; allow slack time for resolution of unintended events; and ensure that critical tasks are completed or justification is provided if project tasks or schedules are not to be completed or are delayed.

Management Response:
Responsible Official:
Raghav Vajjhala

Action Plan:
Management concurs with this recommendation. Through the OCIO re-organization, the CIO has already communicated to all staff the need to obtain skills in Clinger-Cohen

competencies, which include program and project management. Additionally, the CIO has already authorized one telework day a month for all staff to engage in training for the competencies. Lastly, OCIO managers will offer individual training plans to each employee, which will include the recommendation to complete project management training. The individual training plans will identify the skills necessary to plan and manage projects within the FTC environment

Expected Completion:
FY2017 Q2

OIG Analysis: The FTC's planned actions are responsive to our recommendation and, if implemented effectively, would address the objective of our recommendation.

Recommendation 15: *To ensure that FTC sensitive information practices are in place and compliant with federal requirements, the FTC should include CUI program requirements as a topic for consideration in all information systems planning. Specifically, the FTC should:*

Identify systems that may include CUI using FTC policy effective on the date a project is submitted for approval. Include control requirements of the CUI program as identified in NIST Special Publications in FTC planning for systems, information inventories, and information protection controls. Monitor ongoing NARA and NIST CUI program activities to ensure the FTC remains current with the direction and status of CUI program requirements.

Management Response:
Responsible Official:
Raghav Vajjhala & Jeffrey Nakrin

Action Plan:
Management concurs with this recommendation. OCIO has already started the process of revising the Risk Management and Governance policy and will integrate the requirement to identify systems that may include CUI. Additionally, our FISMA inventory database will be revised to include a CUI type indicator and our policies will be revised to assure that the control requirements of the CUI program as identified in NIST security Special Publications are taken into consideration when planning for systems and selecting information safeguard controls. The Records and Filings Office will continue to monitor NARA and NIST CUI program activities and alert agency officials of changes that affect the agency's approach to managing CUI on its systems.

Expected Completion:
CPIC Policy Revision FY2017 Q1
FISMA Inventory Database Revision FY2017 Q1
Policy Revision to incorporate CUI controls FY2017 Q2

OIG Analysis: Recommendation 15 was overtaken by events. The National Archives and Records Administration (NARA) published its CUI Final Rule in the Federal Register on September 14, 2016, and is effective November 14, 2016.