

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 27
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 28
TO EXPERT REPORT OF DR. ERIC B. COLE**

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 29
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/24/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/23/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/24/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/23/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	1/29/2013 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/24/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/23/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/23/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/24/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	10/24/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/23/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/23/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/23/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/23/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/23/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/23/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/23/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/23/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/24/2012 0:00	KB2655992	Security Update	http://support.microsoft.com/?kbid=2655992	CVE-2012-1870
	10/24/2012 0:00	KB2655992	Security Update	http://support.microsoft.com/?kbid=2655992	CVE-2012-1870
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	11/28/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/26/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/25/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/26/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/25/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/26/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/25/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/25/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/26/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/27/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/25/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/25/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
1/25/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007	

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/25/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
REDACTED	1/25/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/25/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
REDACTED	1/25/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
REDACTED	1/25/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
REDACTED	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
REDACTED	10/17/2012 0:00	KB2655992	Security Update	http://support.microsoft.com/?kbid=2655992	CVE-2012-1870
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	11/13/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	11/13/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	1/29/2013 0:00	KB2659262	Security Update for Windows Server 2003 (KB2659262)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	1/29/2013 0:00	KB2676562	Security Update for Windows Server 2003 (KB2676562)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	1/29/2013 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/24/2012 0:00	KB2685939	Security Update	http://support.microsoft.com/?kbid=2685939	CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	1/29/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	1/29/2013 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	1/29/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	11/28/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	1/29/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	1/29/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/29/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
	10/10/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/23/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/10/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/23/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
	10/10/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/23/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/23/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/10/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	10/4/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/23/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/23/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/23/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/23/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/23/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/23/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/23/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/23/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/29/2013 0:00	KB2686509	Security Update for Windows Server 2003 (KB2686509)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	1/29/2013 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/24/2012 0:00	KB2691442	Security Update	http://support.microsoft.com/?kbid=2691442	CVE-2012-0175
	10/24/2012 0:00	KB2691442	Security Update	http://support.microsoft.com/?kbid=2691442	CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	9/25/2012 0:00	KB2479943	Security Update	http://support.microsoft.com/?kbid=2479943	CVE-2011-0032,CVE-2011-0042
	9/25/2012 0:00	KB2660649	Security Update	http://support.microsoft.com/?kbid=2660649	CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	10/24/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	9/25/2012 0:00	KB2706045	Security Update	http://support.microsoft.com/?kbid=2706045	CVE-2012-2523
	1/13/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/24/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/13/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/24/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/23/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/23/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/24/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/25/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/13/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/23/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/23/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/13/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/13/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/13/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/23/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/13/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	11/28/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/17/2012 0:00	KB2691442	Security Update	http://support.microsoft.com/?kbid=2691442	CVE-2012-0175
	1/29/2013 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	10/24/2012 0:00	KB2698365	Security Update	http://support.microsoft.com/?kbid=2698365	CVE-2012-1891
	10/24/2012 0:00	KB2698365	Security Update	http://support.microsoft.com/?kbid=2698365	CVE-2012-1891
	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	10/26/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/19/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/26/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/19/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	10/26/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/19/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/19/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/26/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/27/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/19/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/19/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/19/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/19/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/19/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/19/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/19/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/19/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	11/28/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	10/17/2012 0:00	KB2698365	Security Update	http://support.microsoft.com/?kbid=2698365	CVE-2012-1891
REDACTED	1/29/2013 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/24/2012 0:00	KB2712808	Security Update	http://support.microsoft.com/?kbid=2712808	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	10/24/2012 0:00	KB2712808	Security Update	http://support.microsoft.com/?kbid=2712808	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	11/28/2012 0:00	KB2712808	Security Update	http://support.microsoft.com/?kbid=2712808	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/28/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/17/2012 0:00	KB2712808	Security Update	http://support.microsoft.com/?kbid=2712808	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/29/2013 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/24/2012 0:00	KB2719985	Security Update	http://support.microsoft.com/?kbid=2719985	CVE-2012-1889
	9/25/2012 0:00	KB2530548	Security Update	http://support.microsoft.com/?kbid=2530548	CVE-2011-1246,CVE-2011-1250,CVE-2011-1251,CVE-2011-1252,CVE-2011-1254,CVE-2011-1255,CVE-2011-1256,CVE-2011-1258,CVE-2011-1260,CVE-2011-1261,CVE-2011-1262
	10/24/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/25/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/24/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/25/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	10/24/2012 0:00	KB2719985	Security Update	http://support.microsoft.com/?kbid=2719985	CVE-2012-1889
	10/24/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/25/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/25/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/24/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/25/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/25/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/25/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/25/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/25/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/25/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/25/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/25/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/25/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	11/28/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	3/29/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/17/2012 0:00	KB2719985	Security Update	http://support.microsoft.com/?kbid=2719985	CVE-2012-1889
	10/24/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/25/2013 0:00	KB2716513	Security Update	http://support.microsoft.com/?kbid=2716513	CVE-2012-2531,CVE-2012-2532
	1/25/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/24/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/23/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	10/24/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/25/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/25/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/24/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/25/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/25/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/25/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/25/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/25/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/25/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/25/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/25/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/25/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/25/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/23/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/13/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/19/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/25/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/25/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	3/29/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	1/25/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	9/27/2012 0:00	KB2530548	Security Update	http://support.microsoft.com/?kbid=2530548	CVE-2011-1246,CVE-2011-1250,CVE-2011-1251,CVE-2011-1252,CVE-2011-1254,CVE-2011-1255,CVE-2011-1256,CVE-2011-1258,CVE-2011-1260,CVE-2011-1261,CVE-2011-1262,CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/26/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-2531,CVE-2012-2532
	1/25/2013 0:00	KB2716513	Security Update	http://support.microsoft.com/?kbid=2716513	CVE-2012-2531,CVE-2012-2532
	1/25/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/26/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	10/26/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/25/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/25/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/26/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	1/25/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/25/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/25/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/25/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/25/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/25/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/25/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/25/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/15/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/15/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/25/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/22/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	3/29/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	2/12/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/16/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	10/11/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	12/14/2012 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/11/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	3/21/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	10/11/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/23/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/23/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/11/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/25/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/23/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/23/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/23/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/23/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/30/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/30/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	10/11/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	12/14/2012 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/11/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	1/16/2013 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	10/11/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/23/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/23/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/11/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/23/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/23/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/23/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/23/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	12/14/2012 0:00	KB2729452	Security Update	http://support.microsoft.com/?kbid=2729452	CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	1/29/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	12/14/2012 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/11/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/11/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	12/21/2012 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/11/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/11/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/11/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004	

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/29/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	2/15/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	10/24/2012 0:00	KB2656373	Security Update	http://support.microsoft.com/?kbid=2656373	CVE-2012-0163
REDACTED	10/25/2012 0:00	KB2667402	Security Update	http://support.microsoft.com/?kbid=2667402	CVE-2012-0002,CVE-2012-0152
REDACTED	3/27/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	10/24/2012 0:00	KB2686831	Security Update	http://support.microsoft.com/?kbid=2686831	CVE-2012-1855
REDACTED	3/29/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/27/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	10/24/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/27/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/29/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	10/24/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	10/24/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	1/15/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	10/24/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	10/24/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	1/15/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
REDACTED	1/15/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
REDACTED	1/15/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
REDACTED	1/15/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/15/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
REDACTED	1/15/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
REDACTED	1/15/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
REDACTED	3/29/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277

REDACTED

CSName	InstalledOn	HotFixID	Description	Caption	CVE
	3/29/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/29/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	2/15/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/27/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/27/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/27/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030

REDACTED

CSName	InstalledOn	HotFixID	Description	Caption	CVE
	2/15/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	2/22/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/14/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	1/15/2013 0:00	KB2479943	Security Update	http://support.microsoft.com/?kbid=2479943	CVE-2011-0032,CVE-2011-0042
	1/15/2013 0:00	KB2660649	Security Update	http://support.microsoft.com/?kbid=2660649	CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	1/15/2013 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/15/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	1/15/2013 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/15/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	3/15/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	1/15/2013 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	1/15/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/15/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/15/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/15/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/15/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/15/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/15/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	10/24/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	1/25/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532

REDACTED

CSName	InstalledOn	HotFixID	Description	Caption	CVE
	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	10/24/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	10/24/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/25/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/25/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/24/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	10/24/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/25/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/25/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/25/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/25/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/25/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/25/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/25/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/25/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/14/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/15/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	2/15/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/15/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/15/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/27/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
REDACTED	3/7/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/21/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	2/15/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	1/23/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	1/11/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	12/21/2012 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
REDACTED	1/11/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
REDACTED	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
REDACTED	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
REDACTED	1/11/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
REDACTED	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
REDACTED	1/25/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/23/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/23/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/19/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/25/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/25/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/25/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	2/15/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	1/23/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/23/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/11/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	10/12/2012 0:00	KB2479943	Security Update	http://support.microsoft.com/?kbid=2479943	CVE-2011-0032,CVE-2011-0042
	10/12/2012 0:00	KB2660649	Security Update	http://support.microsoft.com/?kbid=2660649	CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	1/15/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/11/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/11/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	12/21/2012 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/11/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/11/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/11/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/25/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/11/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/11/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/22/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	2/12/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/11/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/16/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	2/22/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	2/22/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	1/18/2013 0:00	KB2799329	Security Update	http://support.microsoft.com/?kbid=2799329	CVE-2012-4792
	1/11/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/30/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	1/29/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	1/22/2013 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	2/4/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	1/22/2013 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/13/2013 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	1/22/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/22/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	2/4/2013 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	1/22/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/22/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	2/4/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/22/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/22/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	2/4/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	2/4/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	1/15/2013 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	3/14/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	11/28/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	2/12/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	11/28/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	2/12/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	11/28/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	2/12/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	2/12/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	11/28/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	11/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	2/12/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	2/12/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	2/12/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	2/12/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	2/12/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	2/12/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	3/15/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	2/12/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2013-0008
	1/23/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/25/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/23/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/15/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/23/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/19/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/25/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	11/28/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/15/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	11/28/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	3/14/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/14/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/15/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
	3/14/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	3/14/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	1/25/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/15/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	1/25/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/23/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	11/28/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/15/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	11/28/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	11/28/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/14/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/15/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
	3/14/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	3/14/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	1/23/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/15/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	1/11/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/15/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	11/28/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/15/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	11/28/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	11/28/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/14/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/15/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
	3/14/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	11/28/2012 0:00	KB2761226	Security Update for Windows Server 2003 (KB2761226)		CVE-2012-2530,CVE-2012-2553,CVE-2012-2897
	3/14/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	1/25/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/15/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	1/11/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/11/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/22/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	2/12/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	1/11/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/16/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	3/21/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/11/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	1/30/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	3/27/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/29/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
	3/27/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/27/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/29/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/29/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/29/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/29/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	2/15/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/27/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/27/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	2/15/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	2/22/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	3/14/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/15/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
	2/15/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/7/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/21/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	2/15/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	3/27/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/29/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/27/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/27/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/29/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/29/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/29/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/29/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	2/15/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
	3/27/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/27/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	2/15/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	2/22/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/14/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/15/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	2/15/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/7/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/21/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	2/15/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	3/27/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	3/29/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	3/27/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
	3/27/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/29/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	3/29/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/29/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	3/29/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	2/15/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	3/27/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	3/27/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	2/15/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	2/22/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	3/14/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/15/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	2/15/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	3/7/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/21/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	2/15/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
REDACTED	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	1/29/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	11/28/2012 0:00	KB2706045-IE8	Security Update for Windows Internet Explorer 8 (KB2706045)		CVE-2012-2523
REDACTED	3/14/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	3/27/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/29/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/27/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/14/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	3/27/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/29/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/14/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/14/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/14/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
	3/14/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	3/14/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/14/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	3/29/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/29/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	10/10/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/15/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	10/10/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	3/15/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/15/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/15/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
	3/15/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	3/15/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/29/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	2/15/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/27/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	12/14/2012 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	3/27/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/11/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/11/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	12/21/2012 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/11/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/11/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/11/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	2/22/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	2/22/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/14/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	2/15/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	2/22/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	10/12/2012 0:00	KB2706045-IE8	Security Update for Windows Internet Explorer 8 (KB2706045)		CVE-2012-2523
	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/15/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/14/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	2/15/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/15/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	3/15/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/15/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
REDACTED	3/15/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/15/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/15/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/15/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/7/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/21/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	10/12/2012 0:00	KB2706045-IE8	Security Update for Windows Internet Explorer 8 (KB2706045)		CVE-2012-2523
REDACTED	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	3/15/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	3/15/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	2/15/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/27/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	3/29/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	3/27/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/27/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	3/29/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/15/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	3/15/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/15/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
REDACTED	3/15/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/15/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	3/15/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/29/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	3/29/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/16/2013 0:00	KB2446710	Security Update	http://support.microsoft.com/?kbid=2446710	CVE-2010-3958
	3/29/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	1/16/2013 0:00	KB2656356	Security Update	http://support.microsoft.com/?kbid=2656356	CVE-2011-3414,CVE-2011-3416,CVE-2011-3417
	3/15/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/27/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	10/17/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	3/27/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	1/16/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
	3/15/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	10/17/2012 0:00	KB2722913	Security Update	http://support.microsoft.com/?kbid=2722913	CVE-2012-1526,CVE-2012-2521,CVE-2012-2522,CVE-2012-2523
	10/17/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	1/16/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	3/22/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	10/17/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/16/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/17/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	10/17/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/16/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/16/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	1/16/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	1/16/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/16/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/16/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	1/16/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	3/14/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/7/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	3/7/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED					2008-4033, CVE-2008-4252, CVE-2008-4253, CVE-2008-4254, CVE-2008-4255, CVE-2008-4256, CVE-2009-0075, CVE-2009-0076, CVE-2009-0090, CVE-2009-0091, CVE-2009-0217, CVE-2009-1547, CVE-2009-2493, CVE-2009-2493, CVE-2009-2497, CVE-2009-2510, CVE-2009-2511, CVE-2009-2524, CVE-2009-2529, CVE-2009-2530, CVE-2009-2531, CVE-2009-3555, CVE-2009-3671, CVE-2009-3672, CVE-2009-3673, CVE-2009-3676, CVE-2009-3678, CVE-2009-4074, CVE-2010-0016, CVE-2010-0017, CVE-2010-0018, CVE-2010-0019, CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0024, CVE-2010-0025, CVE-2010-0026, CVE-2010-0027, CVE-2010-0231, CVE-2010-0232, CVE-2010-0233, CVE-2010-0234, CVE-2010-0235, CVE-2010-0236, CVE-2010-0237, CVE-2010-0238, CVE-2010-0244, CVE-2010-0245, CVE-2010-0246, CVE-2010-0247, CVE-2010-0248, CVE-2010-0249, CVE-2010-0250, CVE-2010-0252, CVE-2010-0265, CVE-2010-0267, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477, CVE-2010-0481, CVE-2010-0482, CVE-2010-0483, CVE-2010-0484, CVE-2010-0485, CVE-2010-0486, CVE-2010-0487, CVE-2010-0488, CVE-2010-0489, CVE-2010-0490, CVE-2010-0491, CVE-2010-0492, CVE-2010-0494, CVE-2010-0805, CVE-2010-0806, CVE-2010-0807, CVE-2010-0808, CVE-2010-0810, CVE-2010-0811, CVE-2010-0816, CVE-2010-0819, CVE-2010-0820, CVE-2010-1255, CVE-2010-1256, CVE-2010-1258, CVE-2010-1263, CVE-2010-1879, CVE-2010-1880, CVE-2010-1883, CVE-2010-1887, CVE-2010-1888, CVE-2010-1889, CVE-2010-1890, CVE-2010-1892, CVE-2010-1893, CVE-2010-1894, CVE-2010-1895, CVE-2010-1896, CVE-2010-1897, CVE-2010-1898, CVE-2010-1899, CVE-2010-2549, CVE-2010-2550, CVE-2010-2551, CVE-2010-2552, CVE-2010-2553,
	11/28/2012 0:00	KB976932	Service Pack	http://support.microsoft.com/?kbid=976932	
	10/10/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850, CVE-2012-1851, CVE-2012-1852, CVE-2012-1853
	10/10/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	3/21/2013 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527, CVE-2012-1528
	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285, CVE-2013-1286, CVE-2013-1287
	10/10/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	3/21/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	3/21/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001, CVE-2013-0002, CVE-2013-0003, CVE-2013-0004
	10/10/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/26/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529, CVE-2012-2546, CVE-2012-2548, CVE-2012-2557, CVE-2012-4969
	3/21/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556, CVE-2012-4786
	3/21/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001, CVE-2013-0002, CVE-2013-0003, CVE-2013-0004
	3/21/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006, CVE-2013-0007
	3/21/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	3/21/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	3/21/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	3/21/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285, CVE-2013-1286, CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285, CVE-2013-1286, CVE-2013-1287

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/15/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/21/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	12/14/2012 0:00	KB2727528	Security Update	http://support.microsoft.com/?kbid=2727528	CVE-2012-1527,CVE-2012-1528
	3/27/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/11/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	12/21/2012 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/11/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/11/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	3/29/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/27/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/27/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/29/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/29/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/29/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	3/29/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	2/15/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	2/15/2013 0:00	KB2797052	Security Update	http://support.microsoft.com/?kbid=2797052	CVE-2013-0030
	1/18/2013 0:00	KB2799329	Security Update	http://support.microsoft.com/?kbid=2799329	CVE-2012-4792
	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/27/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	3/27/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	1/30/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
REDACTED	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	1/30/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
REDACTED	1/30/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	9/28/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	1/30/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
REDACTED	1/30/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
REDACTED	1/30/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/30/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
REDACTED	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	3/14/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/10/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	1/30/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
REDACTED	10/10/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/10/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	1/30/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	10/10/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	9/26/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	1/30/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
REDACTED	1/30/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
REDACTED	1/30/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
REDACTED	1/30/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/30/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
REDACTED	1/30/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
REDACTED	1/30/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
REDACTED	1/30/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/30/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
REDACTED	1/29/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	2/20/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	2/20/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	1/29/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	3/20/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	1/29/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	1/29/2013 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	1/29/2013 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	1/29/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	1/29/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	1/29/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	1/29/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	1/29/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	2/20/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	1/29/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	2/20/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	2/20/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/20/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	1/29/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	2/27/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	2/27/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	1/29/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	10/31/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/31/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/31/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	1/29/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/29/2013 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/31/2012 0:00	KB2718523	Security Update for Windows Server 2003 (KB2718523)		CVE-2012-1890,CVE-2012-1893
	10/31/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	1/29/2013 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	1/29/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	1/29/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/29/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	1/29/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	1/29/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	2/27/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	1/29/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
	2/27/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	2/27/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	1/29/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	2/27/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	2/27/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	1/29/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
	1/29/2013 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	1/29/2013 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	1/29/2013 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/29/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/29/2013 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	1/29/2013 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	1/29/2013 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	1/29/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	1/29/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/29/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	1/29/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	1/29/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	2/27/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	1/29/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
	2/27/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	2/27/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	10/31/2012 0:00	KB2706045-IE8	Security Update for Windows Internet Explorer 8 (KB2706045)		CVE-2012-2523
	10/31/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	1/29/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	1/29/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
	10/31/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	10/31/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	10/31/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	10/31/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/31/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/31/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
	10/31/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/29/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/31/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	1/29/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	1/29/2013 0:00	KB2757638	Security Update for Windows Server 2003 (KB2757638)		CVE-2013-0006,CVE-2013-0007
REDACTED	1/29/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	1/29/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	1/29/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	10/31/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	2/1/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	3/13/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	2/1/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	3/20/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/31/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/31/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/31/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	2/1/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/31/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	2/1/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	2/1/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	2/1/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	2/1/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	2/1/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/20/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	9/26/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	2/1/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	2/1/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	10/10/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	2/1/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	2/1/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	2/1/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	2/1/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	2/1/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	2/1/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	11/2/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	2/1/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	2/1/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	11/2/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/2/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/2/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	2/1/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	11/2/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	2/1/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	2/1/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	2/1/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	2/1/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	2/1/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	9/26/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	2/1/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	2/1/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
	10/17/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	2/1/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	2/1/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	2/1/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	2/1/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	2/1/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	2/1/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
	11/7/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	11/7/2012 0:00	KB2712808	Security Update	http://support.microsoft.com/?kbid=2712808	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	11/7/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	11/7/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	11/7/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	11/7/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	11/13/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	11/13/2012 0:00	KB2698032	Security Update for Windows Server 2003 (KB2698032)		CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	11/13/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	11/13/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	11/13/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	11/13/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	11/13/2012 0:00	KB2761226	Security Update for Windows Server 2003 (KB2761226)		CVE-2012-2530,CVE-2012-2553,CVE-2012-2897
	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	3/8/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/8/2013 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	3/8/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	3/8/2013 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/8/2013 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	3/8/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	11/13/2012 0:00	KB2744842-IE7	Security Update for Windows Internet Explorer 7 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/8/2013 0:00	KB2792100-IE7	Security Update for Windows Internet Explorer 7 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	3/8/2013 0:00	KB2797052-IE7	Security Update for Windows Internet Explorer 7 (KB2797052)		CVE-2013-0030
	11/13/2012 0:00	KB2698032	Security Update for Windows Server 2003 (KB2698032)		CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
	11/13/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	11/13/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	11/13/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
	11/13/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	11/13/2012 0:00	KB2761226	Security Update for Windows Server 2003 (KB2761226)		CVE-2012-2530,CVE-2012-2553,CVE-2012-2897
	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	11/13/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	11/13/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/8/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	11/13/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	11/13/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	11/13/2012 0:00	KB2604078	Security Update for Windows Server 2003 (KB2604078)		CVE-2012-0160,CVE-2012-0161
REDACTED	11/13/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
REDACTED	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	11/13/2012 0:00	KB2659262	Security Update for Windows Server 2003 (KB2659262)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	11/13/2012 0:00	KB2676562	Security Update for Windows Server 2003 (KB2676562)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	11/13/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	11/13/2012 0:00	KB2686509	Security Update for Windows Server 2003 (KB2686509)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	11/13/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
REDACTED	11/13/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	11/13/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
REDACTED	11/13/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/8/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	11/13/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	11/13/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	3/20/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	11/13/2012 0:00	KB2604078	Security Update for Windows Server 2003 (KB2604078)		CVE-2012-0160,CVE-2012-0161
REDACTED	11/13/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
REDACTED	3/21/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	11/13/2012 0:00	KB2659262	Security Update for Windows Server 2003 (KB2659262)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	11/13/2012 0:00	KB2676562	Security Update for Windows Server 2003 (KB2676562)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	11/13/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	11/13/2012 0:00	KB2686509	Security Update for Windows Server 2003 (KB2686509)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
REDACTED	11/13/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
REDACTED	11/13/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	11/13/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
REDACTED	11/13/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/8/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	11/13/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/20/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	11/13/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
	11/13/2012 0:00	KB2604078	Security Update for Windows Server 2003 (KB2604078)		CVE-2012-0160,CVE-2012-0161
	11/13/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
	11/13/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
	11/13/2012 0:00	KB2659262	Security Update for Windows Server 2003 (KB2659262)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	11/13/2012 0:00	KB2676562	Security Update for Windows Server 2003 (KB2676562)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	11/13/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
	11/13/2012 0:00	KB2686509	Security Update for Windows Server 2003 (KB2686509)		CVE-2011-3402,CVE-2012-0159,CVE-2012-0162,CVE-2012-0164,CVE-2012-0165,CVE-2012-0167,CVE-2012-0176,CVE-2012-0180,CVE-2012-0181,CVE-2012-1848
	11/13/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
	11/13/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
	11/13/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	11/13/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	11/13/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
REDACTED	11/13/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/8/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	11/13/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	9/26/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	3/8/2013 0:00	KB2792100-IE8	Security Update for Windows Internet Explorer 8 (KB2792100)		CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
REDACTED	3/8/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	11/13/2012 0:00	KB2698032	Security Update for Windows Server 2003 (KB2698032)		CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
REDACTED	10/10/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	11/13/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	3/8/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	3/8/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/8/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	11/13/2012 0:00	KB2761226	Security Update for Windows Server 2003 (KB2761226)		CVE-2012-2530,CVE-2012-2553,CVE-2012-2897
REDACTED	3/8/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/8/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	3/8/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/8/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	11/15/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	11/15/2012 0:00	KB2698032	Security Update for Windows Server 2003 (KB2698032)		CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
REDACTED	11/15/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	11/15/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	11/15/2012 0:00	KB2761226	Security Update for Windows Server 2003 (KB2761226)		CVE-2012-2530,CVE-2012-2553,CVE-2012-2897
REDACTED	10/10/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	3/20/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	3/20/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	12/7/2012 0:00	KB2698032	Security Update for Windows Server 2003 (KB2698032)		CVE-2012-1895,CVE-2012-1896,CVE-2012-2519,CVE-2012-4776,CVE-2012-4777
REDACTED	10/10/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	12/7/2012 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	3/20/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	3/20/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/20/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	12/7/2012 0:00	KB2761226	Security Update for Windows Server 2003 (KB2761226)		CVE-2012-2530,CVE-2012-2553,CVE-2012-2897
REDACTED	3/20/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/20/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	3/20/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/20/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/20/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	10/10/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	10/10/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	3/20/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	3/20/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/20/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	3/20/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
REDACTED	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
REDACTED	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786
REDACTED	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	10/12/2012 0:00	KB2744842-IE8	Security Update for Windows Internet Explorer 8 (KB2744842)		CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	1/16/2013 0:00	KB2761465-IE8	Security Update for Windows Internet Explorer 8 (KB2761465)		CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	3/13/2013 0:00	KB2797052-IE8	Security Update for Windows Internet Explorer 8 (KB2797052)		CVE-2013-0030
REDACTED	1/16/2013 0:00	KB2799329-IE8	Security Update for Windows Internet Explorer 8 (KB2799329)		CVE-2012-4792
REDACTED	3/13/2013 0:00	KB2809289-IE8	Security Update for Windows Internet Explorer 8 (KB2809289)		CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/12/2012 0:00	KB2655992	Security Update for Windows Server 2003 (KB2655992)		CVE-2012-1870
REDACTED	10/12/2012 0:00	KB2656376-v2	Security Update for Windows Server 2003 (KB2656376-v2)		CVE-2012-0163
REDACTED	10/12/2012 0:00	KB2685939	Security Update for Windows Server 2003 (KB2685939)		CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2691442	Security Update for Windows Server 2003 (KB2691442)		CVE-2012-0175
REDACTED	10/12/2012 0:00	KB2698365	Security Update for Windows Server 2003 (KB2698365)		CVE-2012-1891
REDACTED	10/12/2012 0:00	KB2705219-v2	Security Update for Windows Server 2003 (KB2705219-v2)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2712808	Security Update for Windows Server 2003 (KB2712808)		CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2719985	Security Update for Windows Server 2003 (KB2719985)		CVE-2012-1889
REDACTED	10/12/2012 0:00	KB2724197	Security Update for Windows Server 2003 (KB2724197)		CVE-2012-2529
REDACTED	1/16/2013 0:00	KB2727528	Security Update for Windows Server 2003 (KB2727528)		CVE-2012-1527,CVE-2012-1528
REDACTED	10/12/2012 0:00	KB2731847-v2	Security Update for Windows Server 2003 (KB2731847-v2)		CVE-2012-2527
REDACTED	1/16/2013 0:00	KB2742604	Security Update for Windows Server 2003 (KB2742604)		CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	1/16/2013 0:00	KB2753842-v2	Security Update for Windows Server 2003 (KB2753842-v2)		CVE-2012-2556,CVE-2012-4786

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	1/16/2013 0:00	KB2758857	Security Update for Windows Server 2003 (KB2758857)		CVE-2012-4774
REDACTED	1/16/2013 0:00	KB2770660	Security Update for Windows Server 2003 (KB2770660)		CVE-2012-1537
REDACTED	3/13/2013 0:00	KB2778344	Security Update for Windows Server 2003 (KB2778344)		CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
REDACTED	1/16/2013 0:00	KB2779030	Security Update for Windows Server 2003 (KB2779030)		CVE-2012-2556,CVE-2012-4786
REDACTED	3/13/2013 0:00	KB2780091	Security Update for Windows Server 2003 (KB2780091)		CVE-2013-0077
REDACTED	3/13/2013 0:00	KB2799494	Security Update for Windows Server 2003 (KB2799494)		CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
REDACTED	3/13/2013 0:00	KB2807986	Security Update for Windows Server 2003 (KB2807986)		CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
REDACTED	10/12/2012 0:00	KB2655992	Security Update	http://support.microsoft.com/?kbid=2655992	CVE-2012-1870
REDACTED	10/12/2012 0:00	KB2656373	Security Update	http://support.microsoft.com/?kbid=2656373	CVE-2012-0002,CVE-2012-0152
REDACTED	10/12/2012 0:00	KB2667402	Security Update	http://support.microsoft.com/?kbid=2667402	CVE-2012-0002,CVE-2012-0152
REDACTED	10/12/2012 0:00	KB2685939	Security Update	http://support.microsoft.com/?kbid=2685939	CVE-2012-0173
REDACTED	10/12/2012 0:00	KB2686831	Security Update	http://support.microsoft.com/?kbid=2686831	CVE-2012-1855
REDACTED	10/12/2012 0:00	KB2691442	Security Update	http://support.microsoft.com/?kbid=2691442	CVE-2012-0175
REDACTED	10/12/2012 0:00	KB2698365	Security Update	http://support.microsoft.com/?kbid=2698365	CVE-2012-1891
REDACTED	10/12/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	10/12/2012 0:00	KB2706045	Security Update	http://support.microsoft.com/?kbid=2706045	CVE-2012-2523
REDACTED	10/12/2012 0:00	KB2712808	Security Update	http://support.microsoft.com/?kbid=2712808	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
REDACTED	1/16/2013 0:00	KB2719033	Security Update	http://support.microsoft.com/?kbid=2719033	CVE-2012-2531,CVE-2012-2532
REDACTED	10/12/2012 0:00	KB2719985	Security Update	http://support.microsoft.com/?kbid=2719985	CVE-2012-1889
REDACTED	10/12/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
REDACTED	3/21/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
REDACTED	10/12/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
REDACTED	1/16/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
REDACTED	10/12/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
REDACTED	10/12/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
REDACTED	1/16/2013 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
REDACTED	1/16/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
REDACTED	1/16/2013 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
REDACTED	1/16/2013 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
REDACTED	1/16/2013 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
REDACTED	1/16/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
REDACTED	1/16/2013 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
REDACTED	1/16/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
REDACTED	1/16/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
REDACTED	1/16/2013 0:00	KB2799329	Security Update	http://support.microsoft.com/?kbid=2799329	CVE-2012-4792

CSName	InstalledOn	HotFixID	Description	Caption	CVE
REDACTED	10/11/2012 0:00	KB2705219	Security Update	http://support.microsoft.com/?kbid=2705219	CVE-2012-1850,CVE-2012-1851,CVE-2012-1852,CVE-2012-1853
	10/11/2012 0:00	KB2724197	Security Update	http://support.microsoft.com/?kbid=2724197	CVE-2012-2529
	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288
	10/11/2012 0:00	KB2731847	Security Update	http://support.microsoft.com/?kbid=2731847	CVE-2012-2527
	1/11/2013 0:00	KB2736422	Security Update	http://support.microsoft.com/?kbid=2736422	CVE-2013-0005
	1/11/2013 0:00	KB2742599	Security Update	http://support.microsoft.com/?kbid=2742599	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	10/11/2012 0:00	KB2743555	Security Update	http://support.microsoft.com/?kbid=2743555	CVE-2012-2551
	9/22/2012 0:00	KB2744842	Security Update	http://support.microsoft.com/?kbid=2744842	CVE-2012-1529,CVE-2012-2546,CVE-2012-2548,CVE-2012-2557,CVE-2012-4969
	12/21/2012 0:00	KB2753842	Security Update	http://support.microsoft.com/?kbid=2753842	CVE-2012-2556,CVE-2012-4786
	1/11/2013 0:00	KB2756921	Security Update	http://support.microsoft.com/?kbid=2756921	CVE-2013-0001,CVE-2013-0002,CVE-2013-0003,CVE-2013-0004
	1/11/2013 0:00	KB2757638	Security Update	http://support.microsoft.com/?kbid=2757638	CVE-2013-0006,CVE-2013-0007
	12/14/2012 0:00	KB2758857	Security Update	http://support.microsoft.com/?kbid=2758857	CVE-2012-4774
	12/14/2012 0:00	KB2761465	Security Update	http://support.microsoft.com/?kbid=2761465	CVE-2012-4781,CVE-2012-4782,CVE-2012-4787
	12/14/2012 0:00	KB2765809	Security Update	http://support.microsoft.com/?kbid=2765809	CVE-2012-2549
	1/11/2013 0:00	KB2769369	Security Update	http://support.microsoft.com/?kbid=2769369	CVE-2013-0011
	12/14/2012 0:00	KB2770660	Security Update	http://support.microsoft.com/?kbid=2770660	CVE-2012-1537
	2/15/2013 0:00	KB2778344	Security Update	http://support.microsoft.com/?kbid=2778344	CVE-2013-1248,CVE-2013-1249,CVE-2013-1250,CVE-2013-1251,CVE-2013-1252,CVE-2013-1253,CVE-2013-1254,CVE-2013-1255,CVE-2013-1256,CVE-2013-1257,CVE-2013-1258,CVE-2013-1259,CVE-2013-1260,CVE-2013-1261,CVE-2013-1262,CVE-2013-1263,CVE-2013-1264,CVE-2013-1265,CVE-2013-1266,CVE-2013-1267,CVE-2013-1268,CVE-2013-1269,CVE-2013-1270,CVE-2013-1271,CVE-2013-1272,CVE-2013-1273,CVE-2013-1274,CVE-2013-1275,CVE-2013-1276,CVE-2013-1277
	1/11/2013 0:00	KB2778930	Security Update	http://support.microsoft.com/?kbid=2778930	CVE-2013-0008
	12/14/2012 0:00	KB2779030	Security Update	http://support.microsoft.com/?kbid=2779030	CVE-2012-2556,CVE-2012-4786
	1/11/2013 0:00	KB2785220	Security Update	http://support.microsoft.com/?kbid=2785220	CVE-2013-0013
	2/15/2013 0:00	KB2789645	Security Update	http://support.microsoft.com/?kbid=2789645	CVE-2013-0073
	2/15/2013 0:00	KB2790113	Security Update	http://support.microsoft.com/?kbid=2790113	CVE-2013-0076
	2/15/2013 0:00	KB2790655	Security Update	http://support.microsoft.com/?kbid=2790655	CVE-2013-0075
	2/15/2013 0:00	KB2792100	Security Update	http://support.microsoft.com/?kbid=2792100	CVE-2013-0015,CVE-2013-0018,CVE-2013-0019,CVE-2013-0020,CVE-2013-0021,CVE-2013-0022,CVE-2013-0023,CVE-2013-0024,CVE-2013-0025,CVE-2013-0026,CVE-2013-0027,CVE-2013-0028,CVE-2013-0029
	2/15/2013 0:00	KB2799494	Security Update	http://support.microsoft.com/?kbid=2799494	CVE-2013-1278,CVE-2013-1279,CVE-2013-1280
	3/15/2013 0:00	KB2807986	Security Update	http://support.microsoft.com/?kbid=2807986	CVE-2013-1285,CVE-2013-1286,CVE-2013-1287
	3/15/2013 0:00	KB2809289	Security Update	http://support.microsoft.com/?kbid=2809289	CVE-2013-0087,CVE-2013-0088,CVE-2013-0089,CVE-2013-0090,CVE-2013-0091,CVE-2013-0092,CVE-2013-0093,CVE-2013-0094,CVE-2013-1288

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Wed 16 Jan 2013 02:04:42 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Wed 16 Jan 2013 02:04:42 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Wed 16 Jan 2013 02:04:42 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Wed 16 Jan 2013 02:04:42 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Fri 29 Mar 2013 12:42:14 AM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Fri 29 Mar 2013 12:39:51 AM MST	RHSA-2013:0668	CVE-2012-2677
		Fri 29 Mar 2013 12:39:42 AM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Fri 29 Mar 2013 12:39:40 AM MST	RHSA-2013:0216	CVE-2012-5669
		Fri 29 Mar 2013 12:39:37 AM MST	RHSA-2013:0668	CVE-2012-2677
		Fri 29 Mar 2013 12:39:35 AM MST	RHSA-2013:0568	CVE-2013-0292
		Fri 29 Mar 2013 12:39:13 AM MST	RHSA-2013:0668	CVE-2012-2677
		Fri 29 Mar 2013 12:38:04 AM MST	RHSA-2013:0120	CVE-2012-3417
		Fri 29 Mar 2013 12:37:54 AM MST	RHSA-2013:0123	CVE-2011-4339
		Fri 29 Mar 2013 12:37:39 AM MST	RHSA-2013:0180	CVE-2012-2749 CVE-2012-5611
		Fri 29 Mar 2013 12:37:30 AM MST	RHSA-2013:0568	CVE-2013-0292
		Fri 29 Mar 2013 12:37:26 AM MST	RHSA-2013:0216	CVE-2012-5669
		Fri 29 Mar 2013 12:37:22 AM MST	RHSA-2013:0250	CVE-2012-4545
		Fri 29 Mar 2013 12:37:16 AM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Fri 29 Mar 2013 12:36:53 AM MST	RHSA-2013:0123	CVE-2011-4339
		Fri 29 Mar 2013 12:36:51 AM MST	RHSA-2013:0668	CVE-2012-2677
		Fri 29 Mar 2013 12:36:48 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Fri 29 Mar 2013 12:36:45 AM MST	RHSA-2013:0216	CVE-2012-5669
		Fri 29 Mar 2013 12:36:33 AM MST	RHSA-2013:0568	CVE-2013-0292
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Mon 11 Feb 2013 10:10:42 PM MST	RHSA-2013:0129	CVE-2012-4481 CVE-2012-4522
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3):6(f),(b)(4)	Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:29:03 PM MST	RHSA-2013:0129	CVE-2012-4481 CVE-2012-4522
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Fri 22 Mar 2013 10:08:36 AM UTC	RHSA-2013:0568	CVE-2013-0292
		Fri 22 Mar 2013 10:08:01 AM UTC	RHSA-2013:0216	CVE-2012-5669
		Fri 22 Mar 2013 10:08:01 AM UTC	RHSA-2013:0568	CVE-2013-0292
		Fri 22 Mar 2013 10:08:00 AM UTC	RHSA-2013:0180	CVE-2012-2749 CVE-2012-5611
		Tue 12 Feb 2013 05:12:20 AM UTC	RHSA-2013:0120	CVE-2012-3417
		Tue 12 Feb 2013 05:12:10 AM UTC	RHSA-2012:0304	CVE-2010-0424
		Tue 12 Feb 2013 05:11:42 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Tue 12 Feb 2013 05:11:37 AM UTC	RHSA-2013:0123	CVE-2011-4339

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Tue 12 Feb 2013 05:11:22 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Tue 12 Feb 2013 05:10:36 AM UTC	RHSA-2012:0523	CVE-2011-3048
		Tue 12 Feb 2013 05:10:35 AM UTC	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Tue 12 Feb 2013 05:10:28 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 25 Mar 2013 02:48:21 PM MST	RHSA-2013:0568	CVE-2013-0292
		Mon 25 Mar 2013 02:47:49 PM MST	RHSA-2013:0180	CVE-2012-2749 CVE-2012-5611
		Mon 25 Mar 2013 02:47:49 PM MST	RHSA-2013:0216	CVE-2012-5669
		Mon 25 Mar 2013 02:47:49 PM MST	RHSA-2013:0568	CVE-2013-0292
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:12:20 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:12:10 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:11:42 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:37 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:22 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:36 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:10:35 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:10:28 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:12:20 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:12:10 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:11:42 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:37 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:22 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:36 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:10:35 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:10:28 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 25 Mar 2013 08:58:14 PM UTC	RHSA-2013:0568	CVE-2013-0292
		Mon 25 Mar 2013 08:57:44 PM UTC	RHSA-2013:0216	CVE-2012-5669
		Mon 25 Mar 2013 08:57:44 PM UTC	RHSA-2013:0568	CVE-2013-0292
		Mon 25 Mar 2013 08:57:43 PM UTC	RHSA-2013:0180	CVE-2012-2749 CVE-2012-5611
		Tue 12 Feb 2013 05:12:20 AM UTC	RHSA-2013:0120	CVE-2012-3417
		Tue 12 Feb 2013 05:12:10 AM UTC	RHSA-2012:0304	CVE-2010-0424
		Tue 12 Feb 2013 05:11:42 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Tue 12 Feb 2013 05:11:37 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Tue 12 Feb 2013 05:11:22 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Tue 12 Feb 2013 05:10:36 AM UTC	RHSA-2012:0523	CVE-2011-3048
		Tue 12 Feb 2013 05:10:35 AM UTC	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Tue 12 Feb 2013 05:10:28 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 07:28:59 AM UTC	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 07:28:51 AM UTC	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 07:28:27 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 07:28:22 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 07:28:08 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 07:27:28 AM UTC	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 07:27:27 AM UTC	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 07:27:21 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:28:59 AM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 12:28:51 AM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 12:28:27 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:22 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:08 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:27:28 AM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 12:27:27 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 12:27:21 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:28:59 AM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 12:28:51 AM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 12:28:27 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:22 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:08 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:27:28 AM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 12:27:27 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 12:27:21 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:28:59 AM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 12:28:51 AM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 12:28:27 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:22 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:08 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:27:28 AM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 12:27:27 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 12:27:21 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:28:59 AM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 12:28:51 AM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 12:28:27 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:22 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:08 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:27:28 AM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 12:27:27 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 12:27:21 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3):6(f),(b)(4)	Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:12:20 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:12:10 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:11:42 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:37 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:22 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:36 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:10:35 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:10:28 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:12:20 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:12:10 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:11:42 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:37 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:22 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:36 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:10:35 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:10:28 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:12:20 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:12:10 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:11:42 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:37 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:11:22 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:36 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:10:35 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:10:28 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Fri 08 Feb 2013 03:28:58 AM UTC	RHSA-2013:0120	CVE-2012-3417
		Fri 08 Feb 2013 03:28:48 AM UTC	RHSA-2012:0304	CVE-2010-0424
		Fri 08 Feb 2013 03:28:17 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Fri 08 Feb 2013 03:28:11 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Fri 08 Feb 2013 03:27:54 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Fri 08 Feb 2013 03:27:05 AM UTC	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Fri 08 Feb 2013 03:27:05 AM UTC	RHSA-2012:0523	CVE-2011-3048
		Fri 08 Feb 2013 03:26:56 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:28:59 AM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 12:28:51 AM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 12:28:27 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:22 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:08 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:27:28 AM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 12:27:27 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 12:27:21 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:28:59 AM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 12:28:51 AM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 12:28:27 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:22 AM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 12:28:08 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 12:27:28 AM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 12:27:27 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 12:27:21 AM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424
		Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 25 Mar 2013 02:07:17 PM MST	RHSA-2013:0526	CVE-2012-3386
		Mon 25 Mar 2013 02:05:52 PM MST	RHSA-2013:0589	CVE-2013-0308
		Tue 19 Mar 2013 10:54:19 PM UTC	RHSA-2013:0568	CVE-2013-0292
		Tue 19 Mar 2013 10:53:47 PM UTC	RHSA-2013:0568	CVE-2013-0292
		Tue 19 Mar 2013 10:53:46 PM UTC	RHSA-2013:0180	CVE-2012-2749 CVE-2012-5611
		Tue 19 Mar 2013 10:53:46 PM UTC	RHSA-2013:0216	CVE-2012-5669
		Thu 24 Jan 2013 07:28:59 AM UTC	RHSA-2013:0120	CVE-2012-3417
		Thu 24 Jan 2013 07:28:51 AM UTC	RHSA-2012:0304	CVE-2010-0424
		Thu 24 Jan 2013 07:28:27 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 07:28:22 AM UTC	RHSA-2013:0123	CVE-2011-4339
		Thu 24 Jan 2013 07:28:08 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 24 Jan 2013 07:27:28 AM UTC	RHSA-2012:0523	CVE-2011-3048
		Thu 24 Jan 2013 07:27:27 AM UTC	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 24 Jan 2013 07:27:21 AM UTC	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3):6(f),(b)(4)	Tue 26 Mar 2013 11:46:56 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 11:46:52 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 11:46:03 PM MST	RHSA-2013:0120	CVE-2012-3417
		Tue 26 Mar 2013 11:46:02 PM MST	RHSA-2013:0250	CVE-2012-4545
		Tue 26 Mar 2013 11:45:49 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 11:45:48 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Tue 26 Mar 2013 11:45:42 PM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Tue 26 Mar 2013 11:45:23 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 11:47:56 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 11:47:51 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 11:46:53 PM MST	RHSA-2013:0120	CVE-2012-3417
		Tue 26 Mar 2013 11:46:52 PM MST	RHSA-2013:0250	CVE-2012-4545
		Tue 26 Mar 2013 11:46:35 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 11:46:34 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Tue 26 Mar 2013 11:46:24 PM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Tue 26 Mar 2013 11:46:01 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 11:42:45 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 11:42:41 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 11:41:51 PM MST	RHSA-2013:0250	CVE-2012-4545
		Tue 26 Mar 2013 11:41:48 PM MST	RHSA-2013:0120	CVE-2012-3417
		Tue 26 Mar 2013 11:41:36 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 11:41:35 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Tue 26 Mar 2013 11:41:27 PM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Tue 26 Mar 2013 11:41:01 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 03:07:26 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 03:07:21 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 03:07:20 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Tue 26 Mar 2013 03:06:49 PM MST	RHSA-2013:0250	CVE-2012-4545
		Tue 26 Mar 2013 03:06:48 PM MST	RHSA-2013:0123	CVE-2011-4339
		Tue 26 Mar 2013 03:06:46 PM MST	RHSA-2013:0120	CVE-2012-3417
		Tue 26 Mar 2013 03:06:44 PM MST	RHSA-2012:1255	CVE-2012-2812 CVE-2012-2813 CVE-2012-2814 CVE-2012-2836 CVE-2012-2837 CVE-2012-2840 CVE-2012-2841
		Tue 26 Mar 2013 03:06:40 PM MST	RHSA-2012:1265	CVE-2011-1202 CVE-2011-3970 CVE-2012-2825 CVE-2012-2870 CVE-2012-2871
		Tue 26 Mar 2013 03:06:29 PM MST	RHSA-2013:0123	CVE-2011-4339
		Tue 26 Mar 2013 03:06:29 PM MST	RHSA-2013:0216	CVE-2012-5669
		Tue 26 Mar 2013 03:06:22 PM MST	RHSA-2013:0568	CVE-2013-0292
		Tue 26 Mar 2013 03:06:21 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Tue 26 Mar 2013 03:06:10 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Tue 26 Mar 2013 12:38:01 PM MST	RHSA-2013:0526	CVE-2012-3386
		Tue 26 Mar 2013 12:33:01 PM MST	RHSA-2013:0589	CVE-2013-0308
		Mon 15 Oct 2012 10:46:58 AM MST	RHSA-2012:1269	CVE-2012-2145
		Mon 15 Oct 2012 10:46:00 AM MST	RHSA-2012:1269	CVE-2012-2145
		Mon 11 Feb 2013 10:10:37 PM MST	RHSA-2013:0120	CVE-2012-3417
		Mon 11 Feb 2013 10:10:27 PM MST	RHSA-2012:0304	CVE-2010-0424

Server Name	Update Package	Installed On Date	RHSA	CVE Numbers
REDACTED	(b)(3);6(f),(b)(4)	Mon 11 Feb 2013 10:09:59 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:54 PM MST	RHSA-2013:0123	CVE-2011-4339
		Mon 11 Feb 2013 10:09:39 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Mon 11 Feb 2013 10:08:52 PM MST	RHSA-2012:0523	CVE-2011-3048
		Mon 11 Feb 2013 10:08:44 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Fri 22 Mar 2013 09:32:55 AM MST	RHSA-2013:0135	CVE-2012-2370
		Fri 22 Mar 2013 09:32:52 AM MST	RHSA-2013:0568	CVE-2013-0292
		Fri 22 Mar 2013 09:31:54 AM MST	RHSA-2013:0120	CVE-2012-3417
		Fri 22 Mar 2013 09:31:53 AM MST	RHSA-2013:0250	CVE-2012-4545
		Fri 22 Mar 2013 09:31:42 AM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Fri 22 Mar 2013 09:31:35 AM MST	RHSA-2013:0135	CVE-2012-2370
		Fri 22 Mar 2013 09:31:23 AM MST	RHSA-2013:0568	CVE-2013-0292
		Thu 07 Feb 2013 08:28:58 PM MST	RHSA-2013:0120	CVE-2012-3417
		Thu 07 Feb 2013 08:28:48 PM MST	RHSA-2012:0304	CVE-2010-0424
		Thu 07 Feb 2013 08:28:17 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:28:11 PM MST	RHSA-2013:0123	CVE-2011-4339
		Thu 07 Feb 2013 08:27:54 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2013:0122	CVE-2007-4772 CVE-2007-6067
		Thu 07 Feb 2013 08:27:05 PM MST	RHSA-2012:0523	CVE-2011-3048
		Thu 07 Feb 2013 08:26:56 PM MST	RHSA-2012:0731	CVE-2012-0876 CVE-2012-1148

FTC has submitted 'Cole Att 29 (LIFELOCK-0138079)_Redacted.csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

FTC has submitted 'Cole Att 29 (LIFELOCK-0138080)_Redacted.csv' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 30
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 31
TO EXPERT REPORT OF DR. ERIC B. COLE**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 32
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 33
TO EXPERT REPORT OF DR. ERIC B. COLE**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 34
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

From: Austin Appel [Austin.Appel@lifelock.com]
Sent: Friday, April 26, 2013 6:59 PM
To: David Bridgman; (b)(3);6(f),(b)(4)
Subject: RE: Evidence needed.
Attachments: 2012-11-22 scan.png; 2013-01-03 scan.png; 2013-02-14 scan.png; 2013-03-26 scan.png; SD85254 - med.png; SD85255 - low.png

Well, I might as well write this out now, as my Mondays are generally pretty busy... Keep in mind that this is detailing how I currently rate and evaluate criticality of vulnerabilities based upon the guidelines that Jenner originally set forth. We can evaluate this further to see if changes need to be made.

So, let's start from the point a critical vulnerability is reported by (b)(3);6(f),(b)(4). When evaluating the criticality of the vulnerability, I look for things that may be compensating controls, mitigate the risk, or even just something that is less of a risk to us. The criticality as reported by (b)(3);6(f),(b)(4) and the vendor assumes a worst-case-scenario mentality: service is exposed to the internet and accessible by all. This is (hopefully) not the case within our environment.

There are a number of things that are looked for that can lower a vulnerability's criticality to truly match our own unique environment. To be more detailed, they could include: public accessibility (firewall rules preventing network access externally), internal accessibility (firewall rules preventing network access internally), access restrictions via user accounts, ease of exploitation (public proof-of-concept code/examples, (b)(3);6(f),(b)(4) modules, exploit kits utilizing vulnerability), impact (is it a privilege escalation, denial of service, or remote code execution?), public awareness (lots of news attention?), what is affected, among other aspects at my and the head of the Information Security department's discretion.

Even if a critical vulnerability as rated by CVSS/the developer is downgraded to a medium by our risk analysis, according to our SLAs, it would still need to be remediated within 4 weeks which is still less than the 30 days as required for resolution of a critical vulnerability by PCI.

For this specific system, it is not accessible externally and has limited access internally (as well as other mitigating factors and the nature of these vulnerabilities). Some of these vulnerabilities are rated as medium and some are rated as low. The ones that are rated medium have a higher criticality than the rest due to having public PoC code, a metasploit module, or is being actively used by an exploit pack.

In this case, both the low and medium tickets were submitted on January 28th and were not resolved by the Linux team until April 2nd. It is currently in my queue to verify when the next scan comes along.

Attached are screenshots from multiple (b)(3);6(f),(b)(4) scans and the history of the (b)(3);6(f),(b)(4) tickets. If you need anything else, let me know.

Thanks,

Austin Appel

Information Security Analyst | LifeLock® - Relentlessly Protecting Your Identity™

O: 480.457.2061 | M: (b)(6),(b)(7)

Austin.Appel@lifelock.com

80 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: David Bridgman
Sent: Friday, April 26, 2013 3:47 PM

To: Austin Appel; (b)(3):6(f),(b)(4)
Subject: Evidence needed.

Austin – Apparently the Linux team showed the (b)(3):6(f),(b)(4) their Satellite system and specifically REDACTED which showed Hoyt several critical outstanding patches that are months old. Hoyt would like to see the relating (b)(3):6(f),(b)(4) scans on this system over that time (Since January 1) and the related Tickets. Additionally if we lowered the criticality of the vulnerability he would like to know why and how we came to the level we lowered it to. Can you have this by EOD Monday?

Thanks.

David Bridgman, CISSP
Sr. Information Security Engineer | LifeLock® - Relentlessly Protecting Your Identity™
480.457.2029 Office | (b)(6),(b)(7)(C) Cell
David.Bridgman@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 35
TO EXPERT REPORT OF DR. ERIC B. COLE**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 36
TO EXPERT REPORT OF DR. ERIC B. COLE**

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 37
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.

LODGED UNDER SEAL

FTC PROPOSED ATTACHMENT 38
TO EXPERT REPORT OF DR. ERIC B. COLE

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 39
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

From: (b)(3)6(f),(b)(4)
Sent: Wednesday, April 03, 2013 11:14 AM
To: Austin.Appel@lifelock.com
Subject: Request Id ##84684##, Title Tomcat 5.2.23 Has Multiple Vulnerabilities, has been assigned to you



84684 :: Tomcat 5.2.23 Has Multiple Vulnerabilities - Details

Created by: David Bridgman
Priority: Medium
Due by date: Mar 29, 2013 11:37 AM
Category: Server Support

Description:

During the network pen test the pen testers found that the installed version of tomcat on **REDACTE** has numerous vulnerabilities including multiple denial of service bugs, multiple XSS vulnerabilities and other significant vulnerabilities. While the pen testers scanner detected version 5.5.30 installed according to the banner, this server is actually running version 5.5.23 which has even more vulnerabilities.

Remediation: Upgrade to the latest version of tomcat which is 6.0.36 for **REDACTE**

Here is the list of vulnerabilities with version 5.5.23:

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authen tication	Confiden tiality
1	CVE-2012-5887	287		Bypass	2012-11-17	2012-12-21	5.0	None	Remote	Low	Not required	None
The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and does not properly check for stale nonce values in conjunction with enforcement of proper credentials, which makes it ea attackers to bypass intended access restrictions by sniffing the network for valid requests.												
2	CVE-2012-5886	287		Bypass	2012-11-17	2012-12-21	5.0	None	Remote	Low	Not required	None
The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and caches information about the authenticated user within the session state, which makes it easier for remote attackers to by via vectors related to the session ID.												
3	CVE-2012-5885	264		Bypass	2012-11-17	2012-12-21	5.0	None	Remote	Low	Not required	Partial
The replay-countermeasure functionality in the HTTP Digest Access Authentication implementation in Apache Tomcat 6.x before 6.0.36, and 7.x before 7.0.30 tracks cnonce (aka client nonce) values instead of nonce (aka server nonce) and values, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for vali vulnerability than CVE-2011-1184.												
4	CVE-2012-5568	16		DoS	2012-11-30	2012-12-03	5.0	None	Remote	Low	Not required	None
Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP rec demonstrated by Slowloris.												

5	CVE-2012-0022 189	DoS	2012-01-18	2012-11-06	5.0	None	Remote	Low	Not required	None
Apache Tomcat 5.5.x before 5.5.35, 6.x before 6.0.34, and 7.x before 7.0.23 uses an inefficient approach for handling parameters that allows remote attackers to cause a denial of service (CPU consumption) via a request that contains many parameters and different vulnerability than CVE-2011-4858.										
6	CVE-2011-5064 310	Bypass	2012-01-14	2012-02-15	4.3	None	Remote	Medium	Not required	Partial
DigestAuthenticator.java in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.6.0.33, and 7.x before 7.0.12 uses Catalina as the hard-coded server secret (aka private key), which makes it easier for remote attackers to bypass cryptographic protection mechanisms by leveraging knowledge of this string, a different vulnerability than CVE-2011-1184.										
7	CVE-2011-5063 287	Bypass	2012-01-14	2012-02-15	4.3	None	Remote	Medium	Not required	Partial
The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not check realm values, which might allow remote attackers to bypass intended access restrictions by leveraging the protection space with weaker authentication or authorization requirements, a different vulnerability than CVE-2011-1184.										
8	CVE-2011-5062 264	Bypass	2012-01-14	2012-02-15	5.0	None	Remote	Low	Not required	Partial
The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not check qop values, which might allow remote attackers to bypass intended integrity-protection requirements via a different vulnerability than CVE-2011-1184.										
9	CVE-2011-3190 264	Bypass +Info	2011-08-31	2012-11-06	7.5	None	Remote	Low	Not required	Partial
Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.34, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information via the connector to interpret a request body as a new request.										
10	CVE-2011-2526 20	DoS Bypass	2011-07-14	2012-11-05	4.4	None	Local	Medium	Not required	Partial
Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.19, when sendfile is enabled for the HTTP AJP connector, does not validate certain request attributes, which allows local users to bypass intended file access restriction service (infinite loop or JVM crash) by leveraging an untrusted web application.										
11	CVE-2011-2204 200	+Info	2011-06-29	2012-11-05	4.9	None	Local	Medium	Not required	Partial
Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.17, when the MemoryUserDatabase is used, contains containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information from log file.										
12	CVE-2011-1184 264	Bypass	2012-01-14	2012-02-15	5.0	None	Remote	Low	Not required	Partial
The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nonce (aka client nonce count) values.										
13	CVE-2011-0013 79	XSS	2011-02-18	2012-11-05	4.3	None	Remote	Medium	Not required	None
Multiple cross-site scripting (XSS) vulnerabilities in the HTML Manager Interface in Apache Tomcat 5.5 before 5.5.32, and 7.0 before 7.0.6 allow remote attackers to inject arbitrary web script or HTML, as demonstrated via the display-name parameter.										
14	CVE-2010-3718	Dir. Trav.	2011-02-10	2012-11-05	1.2	None	Local	High	Not required	None

Apache Tomcat 7.0.0 through 7.0.3, 6.0.x, and 5.5.x, when running within a SecurityManager, does not make the Servlet read-only, which allows local web applications to read or write files outside of the intended working directory, as demonstrated by a directory traversal attack.

15	CVE-2010-2227	119	DoS Overflow +Info	2010- 07-13	2011- 10-20	6.4	None	Remote	Low	Not required	Partial
----	-------------------------------	-----	--------------------------	----------------	----------------	-----	------	--------	-----	-----------------	---------

Apache Tomcat 5.5.0 through 5.5.29, 6.0.0 through 6.0.27, and 7.0.0 beta does not properly handle an invalid Transfer-Encoding which allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted request that interferes with "recycling of a buffer."

16	CVE-2010-1157	200	+Info	2010- 04-23	2011- 10-20	6.6	None	Remote	High	Not required	Partial
----	-------------------------------	-----	-------	----------------	----------------	-----	------	--------	------	-----------------	---------

Apache Tomcat 5.5.0 through 5.5.29 and 6.0.0 through 6.0.26 might allow remote attackers to discover the server's host by sending a request for a resource that requires (1) BASIC or (2) DIGEST authentication, and then reading the realm field in the Authenticate header in the reply.

17	CVE-2009-3548	255	+Priv	2009- 11-12	2011- 07-18	7.5	User	Remote	Low	Not required	Partial
----	-------------------------------	-----	-------	----------------	----------------	-----	------	--------	-----	-----------------	---------

The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a password for the administrative user, which allows remote attackers to gain privileges.

18	CVE-2009-2902	22	Dir. Trav.	2010- 01-28	2011- 09-06	4.3	None	Remote	Medium	Not required	None
----	-------------------------------	----	------------	----------------	----------------	-----	------	--------	--------	-----------------	------

Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to read arbitrary directory files via directory traversal sequences in a WAR filename, as demonstrated by the ...war filename.

19	CVE-2009-2901	264	Bypass	2010- 01-28	2011- 02-17	4.3	None	Remote	Medium	Not required	Partial
----	-------------------------------	-----	--------	----------------	----------------	-----	------	--------	--------	-----------------	---------

The autodeployment process in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20, when autoDeploy is enabled, does not remove files that remain from a failed undeploy, which might allow remote attackers to bypass intended authentication requirements.

20	CVE-2009-2693	22	Dir. Trav.	2010- 01-28	2011- 09-06	5.8	None	Remote	Medium	Not required	None
----	-------------------------------	----	------------	----------------	----------------	-----	------	--------	--------	-----------------	------

Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to overwrite arbitrary files via a .. (dot dot) in an entry in a WAR file, as demonstrated by a ../bin/catalina.bat entry.

21	CVE-2009-0783	200	+Info	2009- 06-05	2011- 09-06	4.6	None	Local	Low	Not required	Partial
----	-------------------------------	-----	-------	----------------	----------------	-----	------	-------	-----	-----------------	---------

Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 permits web applications to replace files for other web applications, which allows local users to read or modify the (1) web.xml, (2) context.xml, or (3) tld files of other applications via a crafted application that is loaded earlier than the target application.

22	CVE-2009-0781	79	XSS	2009- 03-09	2011- 09-06	4.3	None	Remote	Medium	Not required	None
----	-------------------------------	----	-----	----------------	----------------	-----	------	--------	--------	-----------------	------

Cross-site scripting (XSS) vulnerability in jsp/cal/cal2.jsp in the calendar application in the examples web application in Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 allows remote attackers to inject arbitrary web script and HTML via the time parameter, related to "invalid HTML."

23	CVE-2009-0580	200	+Info	2009- 06-05	2011- 09-06	4.3	None	Remote	Medium	Not required	Partial
----	-------------------------------	-----	-------	----------------	----------------	-----	------	--------	--------	-----------------	---------

Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when FORM authentication is used, does not properly check for attackers to enumerate valid usernames via requests to /j_security_check with malformed URL encoding of passwords, bypassing error checking in the (1) MemoryRealm, (2) DataSourceRealm, and (3) JDBCRealm authentication realms, as demonstrated by a crafted value for the j_password parameter.

24 [CVE-2009-0033](#) 20 DoS 2009-06-05 2011-09-06 5.0 None Remote Low Not required None

Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18, when the Java AJP connector and load balancing are used, allows remote attackers to cause a denial of service (application outage) via a crafted request with in to temporary blocking of connectors that have encountered errors, as demonstrated by an error involving a malformed H

25 [CVE-2008-5519](#) 200 +Info 2009-04-09 2010-05-04 5.6 None Remote High Not required Partial

The JK Connector (aka mod_jk) 1.2.0 through 1.2.26 in Apache Tomcat allows remote attackers to obtain sensitive info arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that Length header but no POST data or (2) a rapid series of requests, related to noncompliance with the AJP protocol's requ containing Content-Length headers.

26 [CVE-2008-5515](#) 22 Dir. Trav. Bypass 2009-06-16 2011-09-06 5.0 None Remote Low Not required Partial

Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, 6.0.0 through 6.0.18, and possibly earlier versions normalize before filtering the query string when using the RequestDispatcher method, which allows remote attackers to bypass into restrictions and conduct directory traversal attacks via .. (dot dot) sequences and the WEB-INF directory in a Request.

27 [CVE-2008-2370](#) 22 Dir. Trav. 2008-08-03 2010-08-21 5.0 None Remote Low Not required Partial

Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through 6.0.16, when a RequestDispatcher is used, normalization before removing the query string from the URI, which allows remote attackers to conduct directory traver arbitrary files via a .. (dot dot) in a request parameter.

28 [CVE-2008-1947](#) 79 XSS 2008-06-04 2010-08-21 4.3 None Remote Medium Not required None

Cross-site scripting (XSS) vulnerability in Apache Tomcat 5.5.9 through 5.5.26 and 6.0.0 through 6.0.16 allows remote arbitrary web script or HTML via the name parameter (aka the hostname attribute) to host-manager/html/add.

29 [CVE-2008-1232](#) 79 XSS 2008-08-03 2010-08-21 4.3 None Remote Medium Not required None

Cross-site scripting (XSS) vulnerability in Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through attackers to inject arbitrary web script or HTML via a crafted string that is used in the message argument to the HttpServletResponse.sendError method.

30 [CVE-2007-6286](#) 2008-02-11 2009-12-19 4.3 None Remote Medium Not required None

Apache Tomcat 5.5.11 through 5.5.25 and 6.0.0 through 6.0.15, when the native APR connector is used, does not proper request to the SSL port, which allows remote attackers to trigger handling of "a duplicate copy of one of the recent requ by using netcat to send the empty request.

31 [CVE-2007-5342](#) 264 2007-12-27 2010-08-21 6.4 None Remote Low Not required Partial

The default catalina.policy in the JULI logging component in Apache Tomcat 5.5.9 through 5.5.25 and 6.0.0 through 6.0 certain permissions for web applications, which allows attackers to modify logging configuration options and overwrite demonstrated by changing the (1) level, (2) directory, and (3) prefix attributes in the org.apache.juli.FileHandler handler

32 [CVE-2007-5333](#) 200 +Info 2008-02-11 2011-04-20 5.0 None Remote Low Not required Partial

Apache Tomcat 6.0.0 through 6.0.14, 5.5.0 through 5.5.25, and 4.1.0 through 4.1.36 does not properly handle (1) double or (2) %5C (encoded backslash) sequences in a cookie value, which might cause sensitive information such as session ID remote attackers and enable session hijacking attacks. NOTE: this issue exists because of an incomplete fix for CVE-20

33 [CVE-2007-3386](#) 79 XSS 2007-08-14 2010-08-21 4.3 None Remote Medium Not required None

Cross-site scripting (XSS) vulnerability in the Host Manager Servlet for Apache Tomcat 6.0.0 to 6.0.13 and 5.5.0 to 5.5.24 allows attackers to inject arbitrary HTML and web script via crafted requests, as demonstrated using the aliases parameter to ar

34 [CVE-2007-3385](#) [200](#) +Info 2007-08-14 2011-04-20 4.3 None Remote Medium Not required Partial

Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 does not properly handle sequence in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attacker hijacking attacks.

35 [CVE-2007-3382](#) [200](#) +Info 2007-08-14 2010-12-14 4.3 None Remote Medium Not required Partial

Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 treats single quotes (""") cookies, which might cause sensitive information such as session IDs to be leaked and allow remote attackers to conduct attacks.

36 [CVE-2007-2450](#) [79](#) XSS 2007-06-14 2011-03-07 3.5 None Remote Medium Single system None

Multiple cross-site scripting (XSS) vulnerabilities in the (1) Manager and (2) Host Manager web applications in Apache through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote attacker to inject arbitrary web script or HTML via a parameter name to manager/html/upload, and other unspecified vectors.

Link to request: <http://servicedesk.lifelock.com:80/WorkOrder.do?woMode=viewWO&woID=84684>



UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 40
TO EXPERT REPORT OF DR. ERIC B. COLE**

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



SecurityException Risk Assessment Form

RAF # 010
Exp Date: 6/30/14

Vulnerability or Exception Information			
Submitter Name	Andrew Citro	Manager Name	(b)(3)6(f),(b)(4)
Title	Security Engineer	Title	CISO
Date:	10/14/2013		
Host Name(s)	REDACTED	IP Address(es)	
Impact Area(s)			

Description of the Vulnerability or Exception
<p>(b)(3)6(f) alerts (2):</p> <p>1) (b)(3)6 HTTPD: ETag/node information Leakage (CVE-2003-1418) Severity: Severe (4) CVSS: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N) Published: Dec 31, 2003</p> <p>(b)(3)6 HTTP server in certain configurations allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID). Servers: REDACTED</p> <p>2) (b)(3)6 HTTPD: Range header remote DoS (CVE-2011-3192) Severity: Critical (8) CVSS: 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C) Published: Aug 29, 2011</p> <p>A flaw was found in the way the (b)(3)6 HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header. This could be used in a denial of service attack. Advisory: CVE-2011-3192.txt Server: REDACTED</p>

Business Reason for Vulnerability or Exception
<p>Tumbleweed is a self-contained piece of software, meaning they package (b) mysql, and everything else the application uses into their own packages. We are -WAY- out of date on updating Tumbleweed, and have been even when I first started. There was a big push to over-haul and upgrade Tumbleweed, that got cancelled due to the stabilization projects (I was working on the upgrade before the new management came in). The over-haul and upgrade of tumbleweed is a project in itself, because it will affect our end-partners.</p> <p>We can't simply just do an upgrade on the software, because the new versions are not compatible with the older versions, so we would have to step through all of the upgrades in order to get the existing tumbleweed instance upgraded. After speaking to Axway, they said the chances of the upgrades breaking our installation are extremely high, and they recommended that we start with a fresh installation and manually move over the partners and said their newer versions have a better way of handling the upgrades than the previous versions (the one we're using). We are out of true support with the application, because it's reached EOL, but they will still support the basic stuff and help us out. So as long as we don't modify their application, and they do not have patches for the version of tumbleweed that we're running.</p> <p>I can fix the vulnerabilities below, but I would have to modify the software, and then that would void any (even though it's minor right now) support that we have with them. It's on my plate to either replace tumbleweed, or do the upgrade and planning for that is more than likely going to happen towards the end of this year, or at the start of next year. I was truly waiting until the decision was made on (b)(3)6(f),(b)(4) so I could utilize those softwares on the new design/implementation.</p>

Risk Assessment
<p>There is no plan to upgrade Tumbleweed so in the interim, we will plan to mitigate the risk by encrypting the fields as they traverse Tumbleweed.</p> <p>(b)(3)6 HTTP server in certain configurations allows remote attackers to obtain sensitive information via (1) the ETag header, which reveals the inode number, or (2) multipart MIME boundary, which reveals child process IDs (PID).</p>

SecurityException Risk Assessment Form

A flaw was found in the way the (b)(3):6 (b)(4):4 HTTP Server handled Range HTTP headers. A remote attacker could use this flaw to cause httpd to use an excessive amount of memory and CPU time via HTTP requests with a specially-crafted Range header. This could be used in a denial of service attack.

If an attacker takes advantage of these vulnerabilities, he would have access to Highly Confidential information and/or could force the service down with DDOS. The Tumbleweed server is used for critical processes; downtime could cause significant impact the business.

Describe Mitigating Controls

Probability Rating	X	Magnitude of Impact	=	Risk	X	Detection Likelihood Rating	=	RISK RANK	200
1		100		100		2			

Risk Rank Levels: 1-49 = **LOW** Risk Level 50-199 = **MEDIUM** Risk Level >200 = **HIGH** Risk Level

Risk Treatment Plan

The Security Department will present the risk(s) in this RAF to the Security Advisory Group. Because this group meets monthly, RAF forms completed between meetings will be routed to the SAG via email or an adhoc SAG meeting will be called. Use this section to document persons involved in the discussion, select the Agreed upon Risk Treatment Plan, and insert details in the appropriate section.

RECOMMENDATION:

Accept the Risk with Expected Remediation Plan

Accept the Risk with Remediation Plan

Name/Title of Risk Owner	Date of Acceptance
Rich Stebbins/CIO	

Remediation Plan	Owner/Title	Due Date
Encrypt data which traverses Tumbleweed	(b)(3):6(f),(b)(4) CISO	6/30/2014
Upgrade Tumbleweed	(b)(3):6(f),(b)(4) Sr. Director, Infrastructure	TBD (we will reassess risk once (b) is in)

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 41
TO EXPERT REPORT OF DR. ERIC B. COLE**

From: Loretta Stagnitto [loretta@lorettastagnitto.com]
Sent: Monday, May 13, 2013 2:17 PM
To: Rich Stebbins; (b)(3):6(f),(b)(4) Barry.Ghotra@lifelock.com; (b)(3):6(f),(b)(4)
(b)(3):6 Tim Oliver; (b)(3):6(f),(b)(4)
Patrick.Sereno@lifelock.com
Cc: Loretta Stagnitto
Subject: Final VSEM with Shared Goals and SWOT included
Attachments: Final VSEM with goals plus SWOT 5.13.13 (1).ppt; Notes on VSEM & Goals 5.7.13.docx

Hi team – thanks for your participation and leadership during last week’s two sessions with the Infrastructure team. I’m looking forward to getting back together to review the shared goals work plans next week.

Attached is the final VSEM that includes the goals from Q1-Q4, as well as the list of shared goals and work teams we sent out separately, and the combined SWOT from the group’s feedback last week. I integrated them here so we can have a living document that we can continue to reference.

I’ve also attached the notes from the session (mostly 2nd day), that captures some of the ideas the team had to help build trust and communication. If you get together this week during Rich’s staff and have time, you may want to review these and determine what you can incorporate right away.

Thanks again and let me know if you have any questions on the attached. See you next week.

Best wishes,

Loretta



ASSESS. ACT. ACHIEVE.

The "I Know" System for Personal & Team Leadership Development™

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

LifeLock Infrastructure Team

Vision Strategy Execution Metrics

May 2013



2013 LifeLock Company Goals

Member Experience

Develop a best-in-class end-to-end customer experience

- Net Promoter Score: 61%
- Churn: 15%
- Secure Customer Index: 88%

Operational / Infrastructure Efficiency

Create an operating model that will scale with revenue and member growth

- Operating expense to grow as % of revenue growth: 67.2%

Growth

Grow member base and total revenue

- Member base growth: 20%
- Total revenue growth: 31.9%

Culture

Develop an "I make a difference" culture

- Engagement / Recognition metric: 80%
- Undesirable turnover metric: 20%

Infrastructure Team Vision

Enhance the LifeLock member experience and support future membership growth with a high-performing team that will implement a more reliable, secure, and scalable infrastructure platform by the end of 2014.

Strategy – How We Will Achieve the Vision

Technology

Stabilize the current environment

- High availability of infrastructure (always available; business unaware of issues)
 - 99% uptime per system
- Functioning disaster recovery
- Vendor supported versions of technology
- Improved ability/flexibility to support new products quickly
- Confidence in system to handle increased volume
- Comprehensive monitoring and alerting
- Security tools and controls that better protect systems and data and proactively detects security threats and vulnerabilities

Develop a X-year strategic technology plan and roadmap

- Supports short & longer term stabilization strategies outlined above
- Aligns/supports company and business growth objectives & strategies

Processes

Develop business & technology metrics that align with company goals & strategies

- Dashboard & practices for monitoring/refining/realigning

Create key processes for technology operations

- Functioning disaster recovery
- Proactive to detect problems
- Well defined/optimized change management
- Well defined/optimized onboarding & off-boarding of partners
- Well defined/optimized request process
- Well defined/optimized incident management
- Improved ability/flexibility to support new products quickly
- Update InfoSec Policy Manual
- Define or improve technology security standards
- Improve process for security audit log management and process to consistently respond to security alerts and incidents.

People/Culture

Define/build/enhance a high-performing workforce

- Highly functioning teams
 - Minimized conflicts
 - More company-wide collaboration
 - Self-directed issues management
 - Less micromanagement
 - Knowledgeable on environment
 - Functions are directionally aligned
 - LT focuses on bigger issues
- Fewer contractors; FTEs with right skills
- Closer collaboration with engineering & business
 - More time adding functionality than firefighting
- Vehicles for knowledge transfer & cross training of staff
 - Educated on key processes for technology operations
- Better defined organization with workforce plan optimized to current/future needs
 - Better defined application production support
 - Know data and apps
 - Better separation of duties
 - Security minded individuals

Create a culture of collaboration

- Commitment to vision & strategies
- Improved employee satisfaction
- Improved engagement/retention
- Employee investment plans
- I Make A Difference company culture

Execution – Rich’s Goals

Member Experience	Operational/ Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an “I make a difference” culture</p>
<p>Net Promoter Score: 61% Churn: 15% Secure Customer Index: 88%</p>	<p>Operating expense to grow as % of revenue growth: 67.2%</p>	<p>Member base growth: 20% Total revenue growth: 31.9%</p>	<p>Engagement/Recognition metric: 80% Undesirable turnover metric: 20%</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products</p>	<p>Increase stability to improve quality of systems deployed; increase efficiency in Engineering, QA and Release Management; reduce support needs from Infrastructure</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover; increase skill levels; improve teamwork</p>
<p>Cisco/Wsi Integration Other System Changes as required</p>	<p>Systems Stabilization</p>	<p>Re-Architect Systems for Scalability</p>	<p>Organizational Stabilization</p>

Network Goals – Q1 & Q2

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p> <p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Create an operating model that will scale with revenue and member growth</p> <p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Grow member base and total revenue</p> <p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Develop an "I make a difference" culture</p> <p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
<p>Cisco / Wsi Integration Other System Changes as Required</p> <p>Q1. Complete SIP POC to eliminate Cisco/Genesys integration issues.</p> <p>Q1. Implement QoS project – Phase 1 (VoIP)</p> <p>Q2. Implement SIP on CallCenter phones support short-term needs</p> <p>Q2. Review CallCenter RFP Responses and provide feedback.</p> <p>Q2. MPLS Turn-Up for Corporate and 20M to Partner Cloud.</p>	<p>Systems Stabilization</p> <p>Q1. Upgrade Network hardware and software.</p> <p>Q2. Implement New Cluster Landscape</p> <p>Q1. Upgrade core router.</p> <p>Q2. Implement Monitoring Phase 1 project (AP)</p> <p>Q2. Upgrade WiFi @ HQ</p> <p>Q2. Pilot NAC Replacement</p> <p>Q2. Implement Optimization project.</p>	<p>Re-Architect Systems for Scalability</p> <p>Q1. Sunnyvale Turn-Up</p> <p>Q1. Expand Irvine Office Space and WAN</p> <p>Q2. Provision Irvine Phones with Local#s/SIP</p>	<p>Organizational Stabilization</p> <p>Q2. Train for Route/Switch/Data Center for FCoE Implementation</p>

Network Goals – Q3 & Q4

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p> <p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Create an operating model that will scale with revenue and member growth</p> <p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Grow member base and total revenue</p> <p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Develop an "I make a difference" culture</p> <p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
<p>Cisco / Wsi Integration Other System Changes as Required</p> <p>Q3. Implement QoS Phase 2 – Application Prioritization</p> <p>Q4. Implement WiFi Phones for CC MOD</p>	<p>Systems Stabilization</p> <p>Q3. Implement NAC Replacement</p> <p>Q3. Implement Network Environments project.</p> <p>Q3. Implement new VPN Solution</p> <p>Q3. Complete Single Points of Failure Analysis & determine next steps and time based on results.</p> <p>Q3. Define monitoring Phase 2</p> <p>Q4. Implement Monitor Phase 2</p> <p>Q4. Resolve Extranet Routing, Data/VoIP, LAN Best Practice Issues</p> <p>Q4. Implement Single Points of Failure Phase 1 project.</p> <p>Q4. Implement Monitoring Phase 2 project.</p>	<p>Re-Architect Systems for Scalability</p> <p>Q3. Expand Current HQ Network</p> <p>Q4. Implement New HQ Network</p>	<p>Organizational Stabilization</p>

Systems Goals – Q1 & Q2

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an "I make a difference" culture</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
Other System Changes as Required	Systems Stabilization	Re-Architect Systems for Scalability	Organizational Stabilization
<p>Q1. Implement AP Performance Improvement project Phases 1-3.</p>	<p>Q2. Implement New Cluster Landscape project.</p>	<p>Q1. Define Scalability, Redundancy, and Failover project & determine timeline.</p>	<p>Q2. Implement clearly defined process for service request & incident management.</p>
<p>Q2. Implement Exchange 2010</p>	<p>Q2. Implement Systems Environments project.</p>	<p>Q2. Implement Scalability, Redundancy, and Failover project Phase 1.</p>	<p>Q2. Implement process & procedure for problem ownership & resolution.</p>
<p>Q2. Implement short-term storage improvement</p>	<p>Q2. Implement Automated Machine Builds project.</p>	<p>Q2. Define Scalability, Redundancy, and Failover project Phase 2.</p>	<p>Q2. Implement clearly defined escalation paths.</p>
	<p>Q2. Implement Monitoring Phase 1 project (AP)</p>	<p>Q2. Define Disaster Recovery plan.</p>	<p>Q2. Cross-train team members</p>
	<p>Q2. Implement Optimization project.</p>		

Systems Goals – Q3 & Q4

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an "I make a difference" culture</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
Other System Changes as Required	Systems Stabilization	Re-Architect Systems for Scalability	Organizational Stabilization
	<p>Q3. Complete Single Points of Failure Analysis & determine next steps and time based on results.</p> <p>Q3. Define Monitoring Phase 2.</p> <p>Q4. Implement Monitoring Phase 2 project.</p> <p>Q4. Implement Single Points of Failure Phase 1 Project</p>	<p>Q3. Implement Scalability, Redundancy, and Failover project Phase 2.</p> <p>Q3. Define Scalability, Redundancy, and Failover project Phase 3.</p> <p>Q3. Implement Disaster Recovery.</p> <p>Q4. Implement long-term storage improvement.</p> <p>Q4. Implement Scalability, Redundancy, and Failover project Phase 3.</p>	<p>Q3. Define & implement root cause analysis process.</p> <p>Q3. Implement new on-call rotation to leverage 7 members in the team</p>

Database Goals – Q1 & Q2

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an "I make a difference" culture</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
<p>Cisco / Wsi Integration Other System Changes as Required</p>	<p>Systems Stabilization</p>	<p>Re-Architect Systems for Scalability</p>	<p>Organizational Stabilization</p>
<p>Q2. Collaborate with Windows and Linux Teams on implementation of Nagios Monitoring on all Servers containing SQLServer or MySQL.</p>	<p>Q2. Implement New Cluster Landscape project.</p>	<p>Q2. Implement Scalability, Redundancy, and Failover project Phase 1.</p>	<p>Q2. Implement clearly defined process for service request & incident management.</p>
	<p>Q2. Implement Monitoring Phase 1 project (AP)</p>	<p>Q2. Define Scalability, Redundancy, and Failover project Phase 2.</p>	<p>Q2. Implement process & procedure for problem ownership & resolution.</p>
	<p>Q2. Implement Optimization project.</p>		<p>Q2. Implement clearly defined escalation paths.</p>
	<p>Q2. Implement Network Client Encryption</p>		<p>Q2. Cross Train Team Members</p>
	<p>Q2. Enable DML Change ability to PCA</p>		

Database Goals – Q3 & Q4

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
Develop a best-in-class end-to-end customer experience	Create an operating model that will scale with revenue and member growth	Grow member base and total revenue	Develop an "I make a difference" culture
Increase stability of systems so MS agents and members have a seamless use of LifeLock products.	Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.	Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.	Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.
Cisco / Wsi Integration Other System Changes as Required	Systems Stabilization	Re-Architect Systems for Scalability	Organizational Stabilization
Q3. Implement 12c Grid Control for Oracle Monitoring	Q3. Implement Active Data Guard for production standby database	Q3. Implement Backup Strategy to reduce backup failures and promote better monitoring.	Q3. Define & implement root cause analysis process.
Q3 Implement Oracle RAC for Dev/QA	Q3. Complete Single Points of Failure Analysis & determine next steps and time based on results.	Q3. Implement Scalability, Redundancy, and Failover project Phase 2.	
Q3. Implement Oracle RAC for Stage	Q4. Create/Implement Database Auditing and Database Security Standards and Procedures, and Database Hardening Standards and Procedures	Q3. Define Scalability, Redundancy, and Failover project Phase 3.	
Q4. Implement Oracle RAC for HA for Production	Q4. Implement Single Points of Failure Phase 1 project.	Q4. Implement Scalability, Redundancy, and Failover project Phase 3.	
Q4. Implement Oracle RAC for Production Standby	Q4. Implement Oracle Partitioning	Q4. Work with Windows, Linux and Network to enable Jumbo Frames for increased performance to DB.	
	Q4. Implement Data Masking	Q4. Validate use of hyper-threading and work with Windows to remove where results are negative to expectations of industry standards	

Middleware Goals – Q1 & Q2

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an "I make a difference" culture</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
<p>Cisco / Wsi Integration Other System Changes as Required</p>	<p>Systems Stabilization</p>	<p>Re-Architect Systems for Scalability</p>	<p>Organizational Stabilization</p>
	<p>Q2. Implement Systems Environments project.</p> <p>Q2. Implement Automated Machine Builds project.</p> <p>Q2. Implement Monitoring Phase 1 project (AP)</p> <p>Q2. Implement Optimization project.</p> <p>Q2. Analyze and complete the POC for (b)(3);6 10.3.6 and (b)(3);6 11.1.1.x</p>	<p>Q1. Define Scalability, Redundancy, and Failover project & determine timeline.</p> <p>Q2. Implement Scalability, Redundancy, and Failover project Phase 1.</p> <p>Q2. Define Scalability, Redundancy, and Failover project Phase 2, and analyze additional scalability and uptime options for Phase 2.</p> <p>Q2. Explore additional feature sets of SOA suite and work with engineering to see the benefits.</p>	<p>Q2. Implement better RCA and incident management process.</p>

Middleware Goals – Q3 & Q4

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an "I make a difference" culture</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
<p>Cisco / Wsi Integration Other System Changes as Required</p>	<p>Systems Stabilization</p>	<p>Re-Architect Systems for Scalability</p>	<p>Organizational Stabilization</p>
	<p>Q3. Define Monitoring Phase 2.</p> <p>Q3. Complete Single Points of Failure Analysis & determine next steps and time based on results.</p> <p>Q3. Implement the (b)(3):6 10.3.6 and (b) 11.1.1.x project.</p> <p>Q4. Implement (b)(3):6(f), (b)(4) for middleware.</p> <p>Q4. Implement Monitoring Phase 2 project.</p> <p>Q4. Implement Single Points of Failure Phase 1 project.</p>	<p>Q3. Implement Scalability, Redundancy, and Failover project Phase 2.</p> <p>Q3. Define Scalability, Redundancy, and Failover project Phase 3.</p> <p>Q4. Implement Scalability, Redundancy, and Failover project Phase 3.</p>	<p>Q3. Team building including cross training and clearly defined primary and secondary resources.</p>

APS / UTS Goals – Q1 & Q2

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p>	<p>Create an operating model that will scale with revenue and member growth</p>	<p>Grow member base and total revenue</p>	<p>Develop an "I make a difference" culture</p>
<p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
Cisco / Wsi Integration Other System Changes as Required	Systems Stabilization	Re-Architect Systems for Scalability	Organizational Stabilization
<p>Q2. Hire CRM Application Implementation Mngr.</p>	<p>Q2. Complete the laptop refresh project</p>	<p>Q1. Support the Ultimate and LifeLock Jr. projects by ensuring the required functionality updates are made to Right Now</p>	<p>Q1-3. Staff APS group to enable productivity (Q1+1, Q2+1, Q3+1)</p>
<p>Q2. Begin CRM requirements process to define project.</p>	<p>Q2. Implement Monitoring Phase 1 project (AP)</p>		<p>Q2. ServiceDesk Enhancements – Adjust problem categories to include APS.</p>
<p>Q2. Hire Billing Implementation Mngr.</p>	<p>Q2. Complete the Citrix upgrade</p>		<p>Q2. ServiceDesk Enhancements – Produce basic support metrics.</p>
<p>Q2. Define Billing 2.0 implementation & timelines.</p>	<p>Q2. Implement SCCM for windows patching and to automate software deployment to the desktops</p>		<p>Q2. Implement clearly defined process for service request & incident management.</p>
			<p>Q2. Implement process & procedure for problem ownership & resolution.</p>
			<p>Q2. Implement clearly defined escalation paths.</p>

APS / UTS Goals – Q3 & Q4

Member Experience	Operational / Infrastructure Efficiency	Growth	Culture
<p>Develop a best-in-class end-to-end customer experience</p> <p>Increase stability of systems so MS agents and members have a seamless use of LifeLock products.</p>	<p>Create an operating model that will scale with revenue and member growth</p> <p>Increase stability to improve quality of systems deployed, increase efficiency in Engineering, QA, and Release Management, & reduce support needs from Infrastructure.</p>	<p>Grow member base and total revenue</p> <p>Increase scalability to enable higher volume of transactions. Enable seamless increases in systems capacity and eliminate disruption in service.</p>	<p>Develop an "I make a difference" culture</p> <p>Increase employee job satisfaction to reduce undesirable turnover, increase skill level, & improve teamwork.</p>
<p>Cisco / Wsi Integration Other System Changes as Required</p> <p>Q3. Define CRM project phases & begin Phase 1.</p> <p>Q3. Implement Billing 2.0 project components as defined in Q2.</p> <p>Q4. Implement CRM Phase 1 components as defined in Q3.</p> <p>Q4. Implement Billing 2.0 components as defined in Q2.</p>	<p>Systems Stabilization</p> <p>Q3. Complete the Citrix expansion project (Member Services and Contact Center).</p> <p>Q3. Upgrade (b)(3);6 to the current release</p> <p>Q3. Complete Single Points of Failure Analysis & determine next steps and time based on results.</p> <p>Q3. Define Monitoring Phase 2.</p> <p>Q3. Implement a solution to standardize and to reduce the effort to manage the MAC computers</p> <p>Q4. Implement Single Points of Failure Phase 1 project.</p> <p>Q4. Implement Monitoring Phase 2 project.</p> <p>Q4. Move HQ to a new location</p>	<p>Re-Architect Systems for Scalability</p>	<p>Organizational Stabilization</p> <p>Q1-3. Staff APS group to enable productivity (Q1+1, Q2+1, Q3+1)</p> <p>Q3. Define & implement root cause analysis process.</p> <p>Q3. Staff APS group to enable productivity (+2)</p>

Security Goals – Q1 & Q2

Member Experience

Develop a best-in-class end-to-end customer experience

Increase stability of systems so MS agents and members have a seamless use of LifeLock products.

Other System Changes as Required

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

Security Goals – Q3 & Q4

Member Experience

Develop a best-in-class end-to-end customer experience

Increase stability of systems so MS agents and members have a seamless use of LifeLock products.

Other System Changes as Required

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

Q2 Shared Goals

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



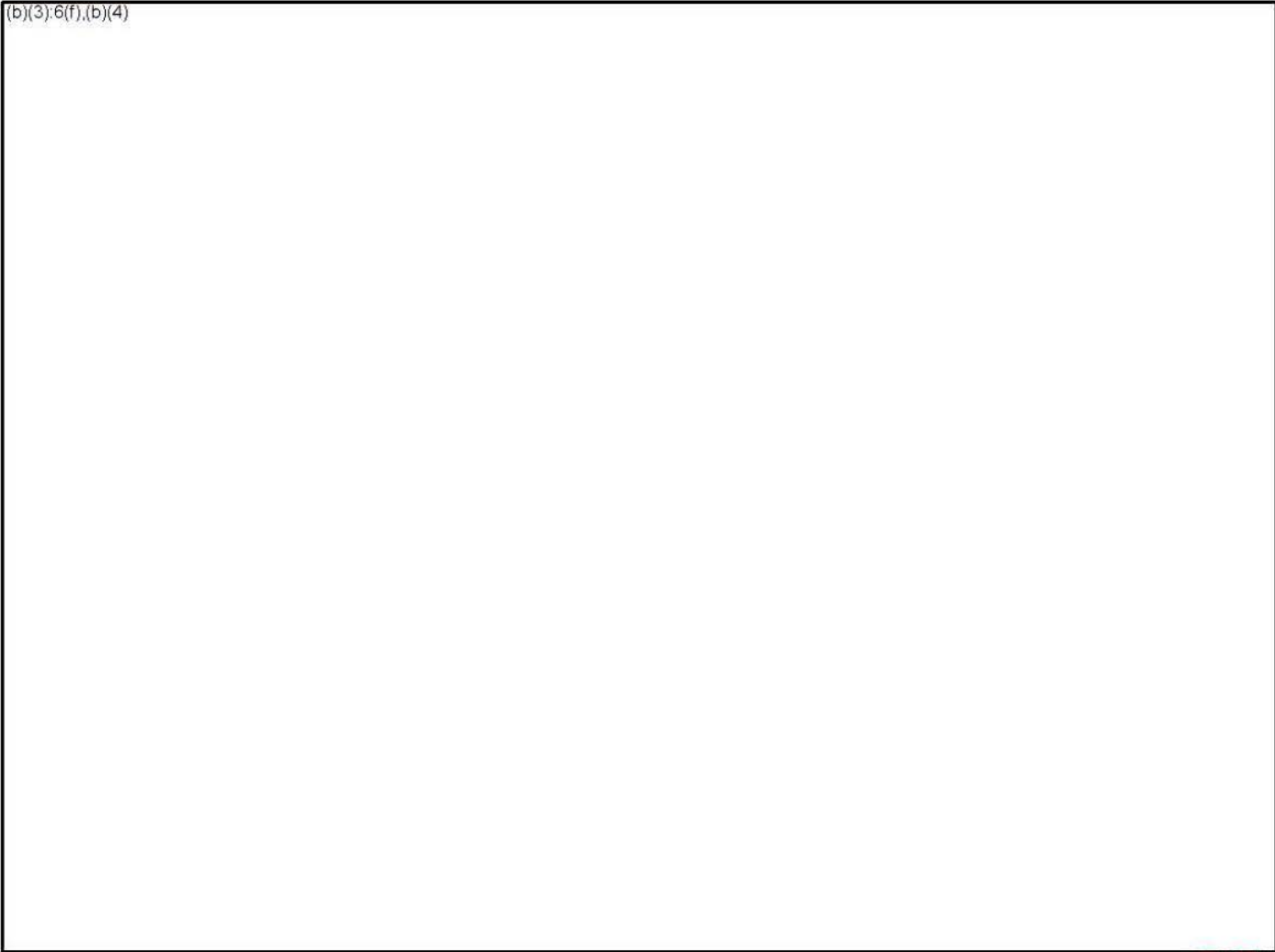
Q2 Shared Goals

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



Q2 Shared Goals

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



Execution & Metrics

- Do our execution plans directly support our vision and strategies?
- What are the milestones for success?
- What are our dependencies?
- How will we measure our success?

Infrastructure Team SWOT - Strengths

- Small/agile/flexible
- Tech competence
- Cohesiveness
- Adaptable
- Action-oriented problem solving
- Knowledge/experience
- Drive/energy
- Execution of tasks
- Technology implementation
- Self awareness (i.e. this training)
- Company resources (\$)
- Innovative thoughts
- People
- Substantial budget
- Exposure to diverse technologies
- Dedicated staff
- Work ethic

Infrastructure Team SWOT - Weaknesses

- Vacancies
- Resource capacity
- No cohesive documentation
- Responsiveness (to each other re: emails, support)
- Work silos (individual teams)
- Too much tribal knowledge
- Not well cross-train of info within teams
- Lack of goals (historically)
- Limited human resources
- Processes/procedures
- Lack of career growth
- Lack of historical knowledge
- Culture
- Leadership
- No cohesive vision
- Understaffed – quantity vs. skills
- Impulsive decision making
- Overly aggressive projects
- No prioritization
- Too accommodating
- Communication
- Trust amongst teams
- Too many contractors
- Speed of deployment
- Representation for outages

Infrastructure Team SWOT – Opportunities

- Growth (company)
- Maturing
 - *Environments*
 - *Teams*
- Scalability
- Improve collaboration
- Improve goal awareness
- Cross training
- Document/improve procedures & standards
- Career building
- Accountability
- Ownership
- Baseline met
- Formal prioritization
- Corporate governance
- Cross team collaboration
- Communication
- Team work
- New infrastructure team (windows)
- Office space
- Team activities/ team building

Infrastructure Team SWOT - Threats

- Many large initiatives at once
- Market competition
 - *Could lose staff*
 - *Can't hire (due to current reputation of LifeLock)*
- Ability to retain staff
- Burn-out
- Morale/buy-in
- Lack of stability
- Security atmosphere – lack of awareness
- Lack of accountability
- High turnover
- Lacking continuity
- Collaboration/cooperation with other departments
- Team cohesion
- Hiring process
- Time
- Vague goals
- Lack of documentation
- Loss of knowledge
- No formal change management activities

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 42
TO EXPERT REPORT OF DR. ERIC B. COLE**

CONFIDENTIAL

From: Andy Doyle [Andy.Doyle@lifelock.com]
Sent: Monday, September 30, 2013 2:45 PM
To: Rich Stebbins
Subject: Goals
Attachments: Infrastructure Goals_Q3_Master October Final.pptx; Goals Summary.xlsx

Rich

Attached you will find 2 files. One is a spreadsheet that has the list of everyone's goals. I extracted these from the deck you sent me a couple of weeks ago. The second is the deck for tomorrow's meeting. We can review both of these at our 5:00.

Andy Doyle
Point B *management consultants*
303.566.0707 / www.pointb.com

LIFELOCK-0077495

Infrastructure

Q3 Shared Goals Status Review

08/28/2013

Objective:

- Update team on progress, risks, dependencies and challenges of shared / Cross-functional goals

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 43
TO EXPERT REPORT OF DR. ERIC B. COLE**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 44
TO EXPERT REPORT OF DR. ERIC B. COLE**

***This Attachment contains excerpted pages only and does not contain all of
the pages in the full bates range of the original document.**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 45
TO EXPERT REPORT OF DR. ERIC B. COLE**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 46
TO EXPERT REPORT OF DR. ERIC B. COLE**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 47
TO EXPERT REPORT OF DR. ERIC B. COLE**

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

December 3, 2014

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This responds to your letter dated November 18, 2014 in which you made follow-up inquiries to our previous submissions relating to LifeLock's information and data security practices. We have set forth the requested information following the order of the requests in your letter. (Please note that your questions are set forth below in bold typeface).

LifeLock Security Incidents

On October 10, 2014, the FTC requested information on two security incidents. LifeLock responded on October 22, 2014 and the FTC is requesting additional information on both security incidents. In addition, the FTC is requesting information regarding a successful penetration test attack.

a. Phishing Emails with Credentials

LifeLock identified a security incident where: "After investigation determined credential compromised for individuals who clicked on a phishing email." LIFELOCK-3173. In LifeLock's October 22, 2014 response, the following employees were identified as having entered their credentials into the malicious website:

(b)(6)

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

For each of these employees please:

- **identify their roles and privileges, including whether any had administrative rights;**
- **identify the applications and categories of documents and files to which they had access rights, and the nature of the access permitted (e.g., read-only or read-write permissions where applicable);**
- **state whether and when they change⁹ their passwords in response to the incident; and**
- **provide logs showing the behavior of their accounts from when their accounts were first compromised to when LifeLock closed the incident.**

Describe any investigation that LifeLock made into the cause of this incident at the time and the results of any such investigation.

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

c. Directory Traversal

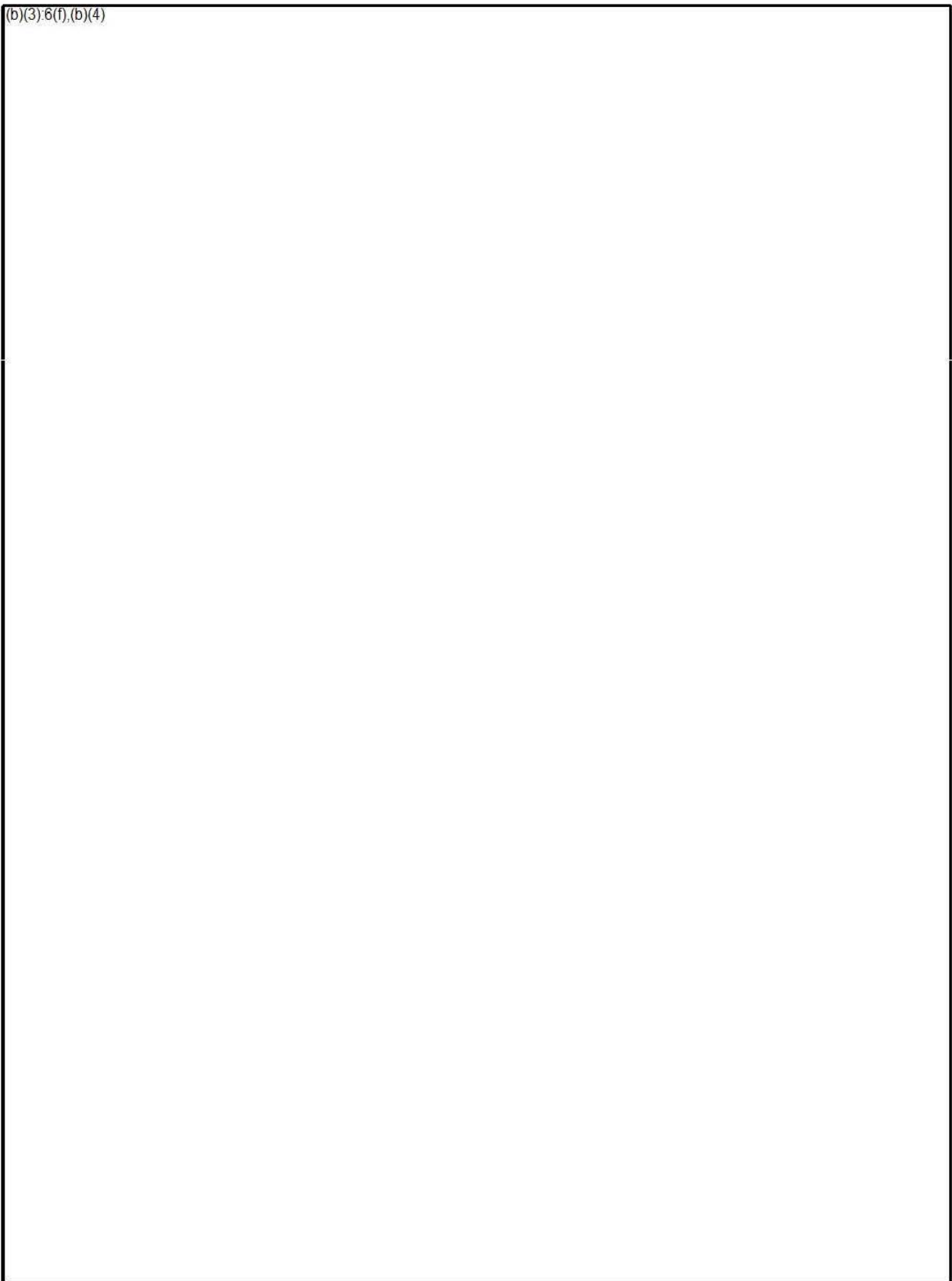
(b)(3):6(f),(b)(4) identified a successful attack scenario in its November 13, 2012 report. LIFELOCK-0053430-37. Included in that report is an identification of some LifeLock employee and member information that was accessed during this attack. *Id.* at 0053435-37, Screenshots.

Identify all LifeLock employee and member information that (b)(3):6(f),(b)(4) was able to access, and all information (b)(3):6(f),(b)(4) would have been able to access, at that time. Include in your response an identification and explanation for each of the data fields that were accessible through this attack scenario. For employee information, identify the roles and privileges, including any administrative rights, that were accessible.

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

(b)(3):6(f),(b)(4) was able to create a user with domain admin rights. With domain admin rights, one has full access (or the ability to give oneself full access) to any Windows system joined to the domain, any fileshare or other systems connected to Active Directory. (b)(3):6(f),(b)(4)

(b)(3), (b)(6), (b)(7)(C), (b)(7)(D)



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

Please advise whether you have any questions regarding the foregoing, and accord the foregoing information and enclosed materials confidential treatment under the Commission's Rules of Practice.

Very truly yours,



Andrew G. Berg
Counsel to LifeLock, Inc.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 48
TO EXPERT REPORT OF DR. ERIC B. COLE**

**LIFELOCK RESPONSE TO FTC 3/13/14 INFORMATION REQUEST --
CONFIDENTIAL TREATMENT REQUESTED**

3. Describe all claims in any advertising or marketing regarding each and every type of alert that will be provided to LifeLock customers.

There are no additional claims responsive to Specification 3 beyond those that were set forth in LifeLock's March 31st response.

11. Describe LifeLock's internal organizational structure for its information security program safeguarding consumers' personal information ("personal information" as defined in the Stipulated Order) from October 2012 to present. Include within your description the date of any changes to the internal organizational structure.

Copies of LifeLock's organizational charts are attached at Annex 11. In general, a new version of the organization charts were created within thirty (30) days of an organizational change which, in general, resulted in a new organizational chart issued on a monthly basis. In addition, title changes and dates associated with promotions or formal job transitions are noted in the table provided in response to Specification 15 below.

12. For the period October 2012 to present, describe the responsibilities and functions of each of the following groups identified on Attachment B, InfoSec Organization table:
- a. Governance, Risk, Compliance
 - b. Security Operations
 - c. Security Technology

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

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

- 13. For the period October 2012 to present, identify each of the groups in Specification No. 12.a-c, whose responsibilities and functions are related to LifeLock's information security program safeguarding consumers' personal information. For each group identified, describe how those responsibilities and functions relate to safeguarding consumers' personal information.**

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

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

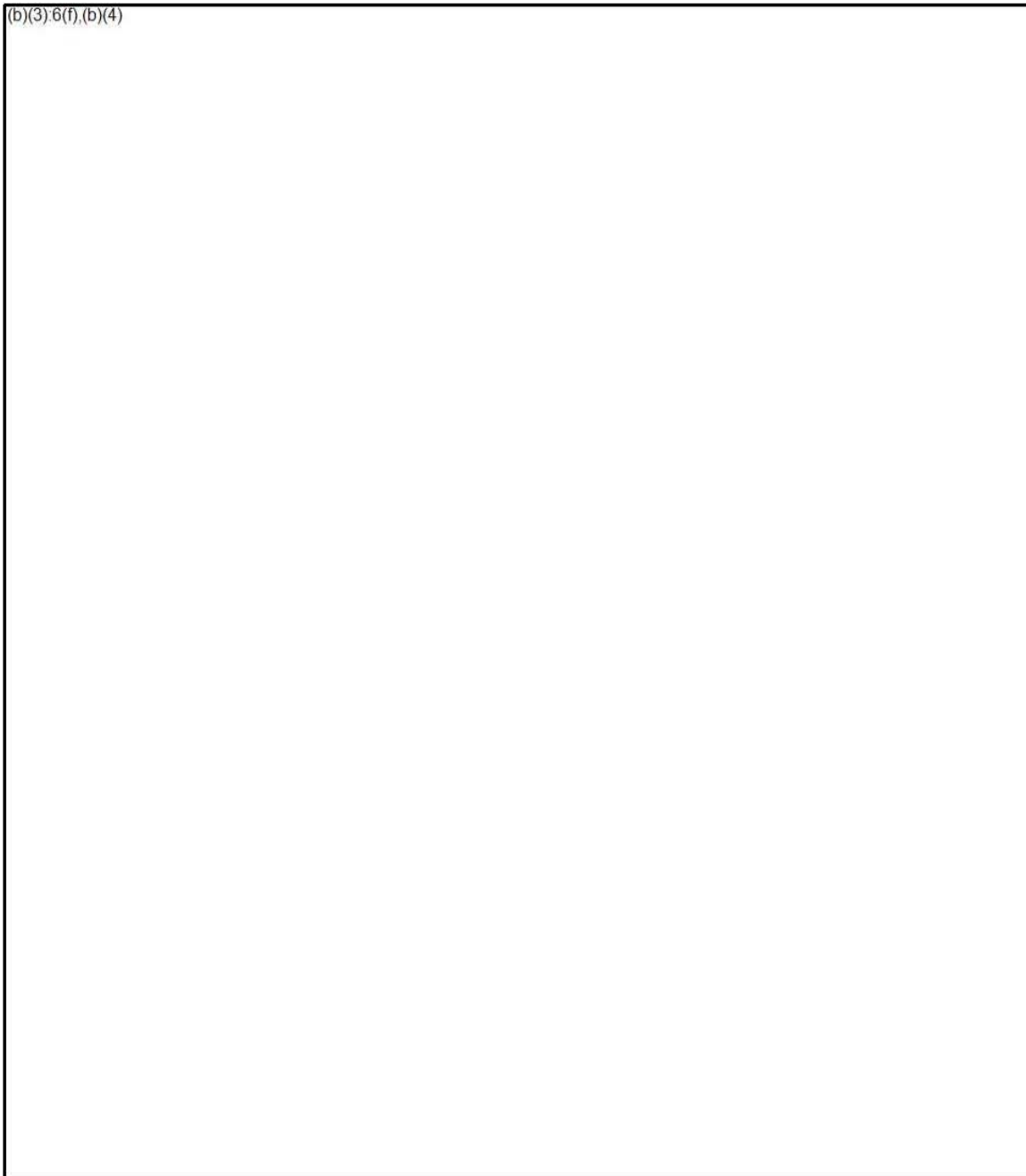
14. Identify all current or past employees, from October 2012 to present, whose job function is, or was, related to LifeLock's information security program for safeguarding consumers' personal information.

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

15. For each employee identified in response to Specification No. 14, provide:
- a. their job title(s) during the period October 2012 to present;

- b. the beginning and ending date for each job they held;
- c. where in the InfoSec Organization structure each job was located; and
- d. the functions related to LifeLock's information security program safeguarding consumers' personal information for each job.

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



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

16. For each job title for each employee identified in response to Specification No. 15.a, estimate the *percentage* of their time spent on job responsibilities involving information security management safeguarding consumers' personal information for each of the periods of time identified in Specification No. 15.b.

See the table below:

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

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

17. Identify all current or past employees, from October 2012 to present, whose *primary* job responsibility is, or was, related to LifeLock's information security program safeguarding consumers' personal information.

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

18. Identify and describe any internal or external information security risk assessments, draft or final, related to LifeLock's information security management safeguarding consumers' personal information conducted since October 2012 to present. Please include any assessments of:
- a. Employee training and management;
 - b. Information systems;
 - c. Prevention or detection of attacks, intrusions, or other systems failures, including vulnerability testing, auditing, monitoring, event logging, awareness education, incident management; and
 - d. Responses to attacks, intrusions, or other systems failures.

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

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

19. Describe LifeLock's continuous monitoring activity for its information security program safeguarding consumers' personal information from October 2012 to the present.

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

20. Describe LifeLock's detection processes for its information security program safeguarding consumers' personal information from October 2012 to the present.

See response to Specification 19 above.

21. Identify and describe any attacks, intrusions, systems failures, or anomalous activity detection related to LifeLock's information security program safeguarding consumers' personal information from October 2012 to present.

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


22. Identify and describe any security breaches or incidents related to LifeLock's information security program safeguarding customers' personal information from October 2012 to present.

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

23. Describe any actions LifeLock undertook in response to any security breaches or incidents identified in response to Specification Nos. 21 and 22.

The table below summarizes the actions LifeLock undertook in response to the security incidents identified in LifeLock's response to Specification 22.

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



- 27. Produce the resumes or qualifications for each of the individuals identified in response to Specification No. 14.**

Responsive documents are set forth in Annex 27.

- 28. Produce the job descriptions for each of the jobs identified in response to Specification No. 15, for the time period from October 2012 to the present.**

Responsive documents are set forth in Annex 28. Certain positions may not have job descriptions available, such as: Chief Legal Officer and General Counsel (Lemon (a temporary position related to a prior acquisition which position has since been eliminated)).

- 31. To the extent not previously produced in response to the above document Request Specifications, produce all documentation supporting the information you have provided in response to Specification Nos. 10-24.**

Responsive documents are set forth in Annex 31.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 49
TO EXPERT REPORT OF DR. ERIC B. COLE**

THE STATE OF SECURITY

News.. Trends.. Insights.



HOME » IT SECURITY AND DATA PROTECTION » PCI DSS Compliance: More Carrot and Less Stick?

PCI DSS Compliance: More Carrot and Less Stick?

CINDY VALLADARES

MAY 17, 2011 |

RISK-BASED SECURITY FOR EXECUTIVES



Or a less sexy title: does compliance with mandates such as Payment Card Industry Data Security Standard (PCI DSS) help reduce risks for organizations (the carrot) even though it's costly and the consequences of non-compliance even costlier (the stick)?

The best politically-correct answer is: it depends on who you are and what your approach to compliance is.

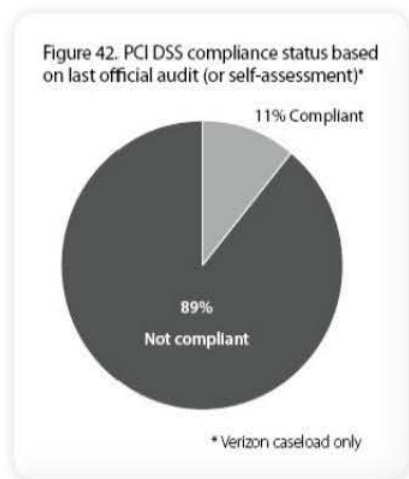
One of the lingering questions from our discussions around PCI in this report is always that of relevancy. It's all well and good to validate compliance with the PCI DSS, but does it actually help reduce risk? Insofar as that translates to a sincere security program—one that seeks to maintain validation on an ongoing basis—the data strongly suggests the answer is “yes.”

Verizon's **2011 Data Breach Investigations Report** points out that PCI DSS compliance is having some positive risk reduction results for organizations, as long as compliance is treated as a continuous process, not a one-time validation exercise.

The State of Security Newsletter +

It is important to clarify this point, since “Compliance is a continuous process of adhering to the regulatory standard,” and

FTC-0002852



“validation . . . is a point-in-time event . . . that attempts to measure and describe the level of adherence to the standard.”

In other words, validation ≠ compliance; compliance ≠ security; thus validation ≠ security. But even validation, as minimalistic to security as it may seem, does show some positive results.

What this graph in the DBIR shows us is that most organizations (89%) that have been breached, were not compliant with PCI DSS at the time of the breach. They might have passed an audit, but were not compliant with the standard when the breach happened.

To fully understand these findings, I strongly encourage you to

read the entire report.

So which organizations benefit most from being compliant with the PCI DSS? In a recent conversation with **Mike Dahn**, he shared the idea that compliance validation only helps organizations that have high security and low maturity (defined as not having documented policies or procedures) — those in group 1 in this chart— and those organizations that have low security and high maturity, those in group 2 of this graph.

Group 3 is a lost cause — they will never care about compliance or security. Group 4 is the *creme de la creme*. These organizations go a step beyond and manage risk (not only security) and see compliance as a nuisance to implementing best practices.

A full review of Mike Dahn's thoughts on this topics can be found on his recent [blogpost](#).

So what does constitute “best in class” in security and risk management? If you haven't read **Josh Corman**'s thoughts on this topic, you should. Most of his antipathy towards compliance is because he believes compliance punishes the visionary and elite practitioner who cares deeply about managing risk. He recently published what I call “Corman's hierarchy of security needs”.

High Security Low Maturity 1	High Security High Maturity 4
Low Security Low Maturity 3	Low Security High Maturity 2

His proposition is that the “compliance is good enough” approach has proven to be insufficient and very risky. And in his pyramid he describes a way organization can do better security.

First, you need to build a defensible infrastructure. As in the

Survival Guide/Pyramid



the 451 group

story of the three little pigs, do you want to build a house made of hay or a brick house?

Secondly, you have to instill some operational discipline. He refers to the work of **Gene Kim** on studying high-performing organizations.

The next step is to build some situational awareness: the ability to

detect threats/risks sooner, understand the impact on the business, and be able to react faster.

Lastly and only then, utilize some countermeasures. I'm not giving this enough justice and I'm not as entertaining in a blogpost as Mr. Corman is in person, so see for yourself in this **recorded version** of his PechaKucha talk during RSA.

I hope this blogpost provides you with some guidance and resources wherever you are in your compliance, security and risk management journey.

Hasta pronto!

@cindyv



CATEGORIES [IT Security and Data Protection](#), [Regulatory Compliance](#), [PCI](#), [Regulatory Compliance](#), [Risk-Based Security for Executives](#), [Risk Management](#), [Risk-Based Security for Executives](#)

TAGS [IT Security](#), [IT Security and Data Protection](#), [PCI](#), [PCI DSS](#), [Regulatory Compliance](#), [_IT Compliance](#)



**WILL THE REAL
FIM Shady please stand up?**

Don't settle for a wannabe.
TRIPWIRE—The undisputed leader in
File Integrity Monitoring for 20 years.

LEARN MORE

RECENT TRACKBACKS

[IT Security, Compliance and Best Practices » Blog archive » How to Achieve Better Security](#)

[...] [PCI DSS Compliance: More Carrot and Less Stick?](#) [Archives](#) [Select Month](#) [June 2011](#) [May 2011](#) [April 2011](#) [March 2011](#) [February 2011](#) [January 2011](#) [December 2010](#) [November 2010](#) [October 2010](#) [September 2010](#) [August 2010](#) [July 2010](#) [June 2010](#) [May 2010](#) [April 2010](#) [March 2010](#) [February 2010](#) [December 2009](#) [November 2009](#) [October 2009](#) [September 2009](#) [August 2009](#) [June 2009](#) [May 2009](#) [April 2009](#) [March 2009](#) [February 2009](#) [January 2009](#) [December 2008](#) [November 2008](#) [October 2008](#) [September 2008](#) [August 2008](#) [July 2008](#) [June 2008](#) [May 2008](#) [Tags](#) [audit](#) [bsides](#) [Change Control](#) [Chris Hoff](#) [Cloud](#) [cloud computing](#) [Compliance](#) [ConfigCheck](#) [data breach](#) [Data Breaches](#) [ESX](#) [event management](#) [File Integrity Monitoring](#) [FIM](#) [Gene Kim](#) [Information Security](#) [Information Security](#) [Infosec](#) [IT Security](#) [ITSM](#) [Josh Corman](#) [log management](#) [microsoft](#) [Mike Dahn](#) [Ninja PCI](#) [PCI DSS](#) [Pirate risk](#) [Risk management](#) [RSA](#) [RSA 2010](#) [RSAC](#) [RSA Conference](#) [Security B-Sides](#) [trends](#) [tripwire](#) [VirtSec](#) [virtualization](#) [VM admins](#) [vmware](#) [What Virtualization, Problem?](#) [_Change Management](#) [_IT Compliance](#) [_Virtualization](#) [Security](#) « [Digesting the 2011 Verizon Data Breach Investigations Report: Best of blogs and podcasts](#) [...]

COMMENTS

Login  

There are no comments posted yet. **Be the first one!**

POST A NEW COMMENT

Comment as a Guest, or login:   

NAME

EMAIL

WEBSITE (OPTIONAL)

FTC-0002855

Displayed next to your comments.

Not displayed publicly.

If you have a website, link to it here.

Subscribe to

Submit Comment

None

About Cindy Valladares



Cindy Valladares has contributed 147 posts to The State of Security.

View all posts by **Cindy Valladares** >

 **Follow @cindyv**

FTC-0002856

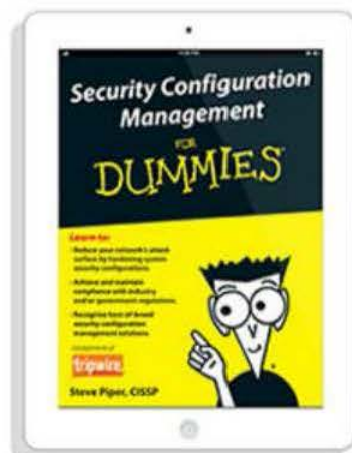


The State of Security Newsletter

Receive the latest security stories, trends and insights directly in your inbox each week.



FREE EBOOK



Security Configuration Management
For Dummies

Download Now

FTC-0002857

Latest Security News

Expedia, Travelocity, Hotels.com Warn Customers of Phishing Scam JUN 25, 2015

Business Email Compromise Scam Alert Issued by FS-ISAC JUN 25, 2015

Industrial Control System (In)Security: Nearly Half of Attacks Go Unattributed JUN 24, 2015

Fake Royal Mail Delivers CryptoLocker Ransomware to Recipients JUN 24, 2015

Uber's Updated Privacy Policy Could Allow It To Track You 24/7 JUN 23, 2015

POPULAR

FEATURED

RECENT



VERT Vuln School: Return-Oriented Programming (ROP) 101

JUNE 23, 2015



Samsung announces fix for major Galaxy keyboard security flaw

JUNE 19, 2015



Hackers Can Use Pita Bread to Steal Laptop Encryption Keys, Say Researchers

JUNE 23, 2015



The 5 Most Common Attack Patterns of 2014

JUNE 24, 2015



The Difference Between Cybersecurity Literacy and Awareness

JUNE 22, 2015

FTC-0002858

Tweets

Follow



Tripwire, Inc. @TripwireInc 10m

Expedia, Travelocity, [Hotels.com](#)
Warn Customers of Phishing Scam
[tripwire.me/1J88pYd](#) via @ritzanti
#infosec #security

Show Summary



Tripwire, Inc. @TripwireInc 37m

The 5 Most Common Attack
Patterns of 2014
[tripwire.me/1LmT7B7](#) via
@DMBisson #security #infosec

Show Summary



HELP NET SECURITY Help Net Security 7h

Tweet to @TripwireInc



Tripwire

You like this.

You and 5,875 others like Tripwire. 5,875 people like Tripwire.



Topics

Government

Incident Detection

[IT Security and Data Protection](#) ▢

[Latest Security News](#) ▢

[Off Topic](#) ▢

[Regulatory Compliance](#) ▢

[Risk-Based Security for Executives](#) ▢

[Security Awareness](#) ▢

[Security Slice](#) ▢

[Tripwire News](#) ▢

[Vulnerability Management](#) ▢

© 2015 TRIPWIRE, INC. ALL RIGHTS RESERVED.

FOLLOW US



**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

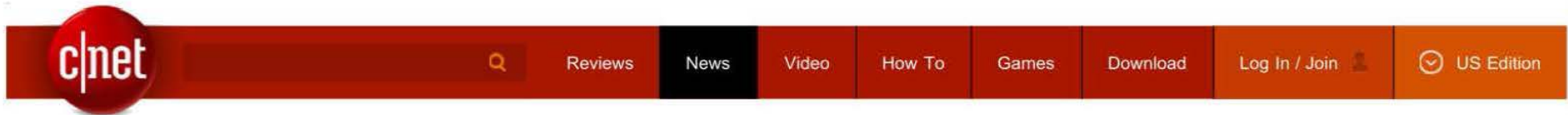
Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 50
TO EXPERT REPORT OF DR. ERIC B. COLE**



CNET > Security > PCI compliance: What it is and why it matters (Q&A)

PCI compliance: What it is and why it matters (Q&A)

Bob Russo, general manager of the PCI Security Standards Council, explains what his organization is doing to keep payment card data out of the hands of criminal hackers.

by **Elinor Mills**  @elinormills / February 8, 2010 4:00 AM PST



If you own a bank account or use credit cards, chances are you've heard the term "PCI

THIS WEEK'S MUST READS /

FTC-0002861

 **PCI compliance: What it is and why**

compliant." But you probably don't know what it means.

The term is heard more and more frequently these days as data breaches at merchants like TJX, parent of TJMaxx, and payment processors **Heartland Payment Systems** and **RBS WorldPay** land millions of card records in the hands of hackers. Criminals are using the data to make purchases and withdraw money from accounts of unsuspecting victims who did nothing wrong; they just owned a card.

It's a huge and growing problem. More than 80 percent of data stolen in breaches is payment card data, according to the **2009 Verizon Business Data Breach Report**.

CNET asked Bob Russo, general manager of the **PCI Security Standards Council**, to explain what is being done to keep criminals from accessing consumer payment card data.

Q: So, what does the PCI Security Standards Council do?

Russo: The council was formed in September 2006 by the five major credit card brands, Visa, MasterCard, American Express, Discover, and JCB [Japanese Credit Bureau]. It was formed because each one of the brands has their own compliance programs and they still do, but they all use this standard as the foundation for their programs. There was a time when you could pick up the phone and call one brand and ask a security question and get one answer and call another brand and ask the same question and get a different answer. They all now use these standards that we manage as the foundation for those compliance questions.

What is the standard exactly?

Russo: It's the PCI, which stands for Payment Card Industry, data security standard. It's a set of 12 specific requirements that cover six different goals. It's very prescriptive. It says not only that you need to be secure but it tells you how to become secure. It's more about security than compliance. The goals are things like build and maintain a secure network, protect card holder data and regularly monitor and test the networks. That's the main standard. We manage three different standards. The first one covers everything from the physical security to logical security.



Bob Russo, general manager of the PCI Security Standards Council.

PCI Security Standards Council

1

it matters (Q&A)

Security /

2

Inside Comic-Con 2015: Drowning in fandom at the vortex of pop culture

Tech Culture /

3

How consumers can fight back against big wireless

Mobile /

4

T-Mobile hints at 'big, bold' plan this week

Mobile /

5

Comcast to launch \$15-per-month streaming TV for cord cutters

Internet /

The second standard is PADSS, Payment Application Data Security Standard. These are for payment applications a merchant would buy off the shelf. For example, if you went to a restaurant and you ordered your meal and the waiter used a touch-screen terminal, that puts the order in the kitchen and it's tied to an ordering database. The application also takes the credit card at the end of the meal. We make sure these applications aren't storing prohibitive data, such as data on the magnetic strip on the card. If they stored that data and someone got a hold of it then they would be able to clone credit cards. There are literally thousands of applications out there and when it's compliant with the standard it gets listed on our Web site.

"We have seen no evidence that if someone were compliant that they would have been breached. The standard is working. You only read about the one or two or four big breaches that happen. You don't hear about the thousands of merchants who aren't getting breached because they are compliant."

--Bob Russo, general manager, PCI Security Standards Council

The last piece we manage is called PTS, PIN Transaction System. Anytime you enter a PIN number, for example, this standard would take effect. It looks at those PIN entry devices so when you go to a large department store and you buy something and you use a debit card they'll hand you a PIN pad and you key in your number. We certify those devices as well as unattended payment terminals, such as those used at gas station [islands], ticket kiosks, and transit systems, like the Boston underground.

There have been a number of big data breaches lately. Were the companies PCI compliant or not in those cases?

Russo: It's been our experience that none of the breaches that occurred have been compliant at the time of the breach. Becoming compliant with the standard is pretty much a snapshot in time. An assessment company would come in and go through all those requirements and check that this stuff is in place. If everything is in place they issue a report on compliance. It is then your responsibility as a merchant to maintain that compliance. If there are new patches to come out for the operating system you have to install those. One piece we ask for is that you turn the logging on. Forensics find all the information in the logs so we insist you turn the logging on. Except, if nobody ever looks at these logs and they're sending out alerts, what good is it? It's up to the merchant to make sure they stay in compliance and that they are secure. For each of those [big public] breaches credit card companies looked at the logs [and found] that none of them was compliant at the time of the breach.

But I thought Heartland executives said they were compliant.

Russo: They had that piece of paper that said they were compliant but they weren't. What happened at Heartland was a SQL injection attack [in which an attacker injects commands to a back end database using input fields on a Web site]. That's an old exploit and there are myriad ways to prevent that outlined in the standards. As it turns out they were not complaint at the time of the breach. [Heartland CEO Robert Carr **eventually disclosed** that the assessors had incorrectly

informed the company that it was PCI compliant.]

But even if the merchant is PCI compliant that doesn't necessarily mean the shop is secure, right?

Russo: Exactly. That's why we say it's about security not compliance.

If that's the case, shouldn't the standard be improved so it is more effective?

Russo: That wasn't the case here. We have seen no evidence that if someone were compliant that they would have been breached. The standard is working. You only read about the one or two or four big breaches that happen. You don't hear about the thousands of merchants who aren't getting breached because they are compliant.

If a merchant is found to be not PCI compliant, what are the consequences?

Russo: Ninety percent of consumers don't understand the difference between credit card fraud and identity theft. If they hear that their credit card has been stolen, like at Heartland or TJX, many of them believe their identity is at risk. If that's the case many of your customers won't shop with you anymore because they are afraid you are not protecting their data and someone is going to steal their identity. That's the worst thing that can happen. The biggest problem would be if your customers walk away. There are reputational damages they have to deal with, which nine times out of 10 cannot be measured in terms of dollars.

There are also fines levied by card brands. There are lawsuits coming out of the woodwork when something like this happens, like shareholder lawsuits and class action customer lawsuits. They are paying to issuing banks for reissuing cards. And the government might now get involved. They're looking to find if stolen credit card information is being used to finance terrorism. You've got myriad people on your back if you suffer a breach. You may have FTC involved, and they require 20 years of audits. Every other year you would have to go through a complete audit. It's very expensive to suffer a breach. It's much better to be compliant and secure and not have to worry about this.

How much are the fines?

Russo: The brands set those; we're not responsible for the fines. We just set the standards and they are enforced by the brands and the federal agencies.

What part of the standard is mandatory and what is voluntary?

Russo: It's all mandatory. Nothing is voluntary. The rule is if you store, process, or transmit credit card data you must be compliant with the PCI standards. And that's a global rule.

What can consumers do to protect themselves?

Russo: Consumers need to take a little bit of responsibility now. You can watch your credit card activity online. I can watch all my credit cards online to see what I'm spending, and what my wife and my kids are spending. You really should be monitoring your credit card statements. If you have to, do it when the statement comes in the mail. If you do it

"Consumers need to take a little bit of responsibility now. You can watch

online you can do it more often and set up alerts via email. Consumers by and large don't have a lot of liability when it comes to credit cards. A lot of credit cards are zero-liability. You just call the company and say this was not my charge and they won't hold you responsible for it.

Debit cards are treated differently than credit cards, right?

Russo: Debit cards are somewhat different. With a debit card you're actually using your own money coming out of your own checking account. The liability will vary depending on the card and the bank.

What are the biggest challenges for the industry?

Russo: Education is a big issue. Some of the smaller merchants that just come into the business don't really know what their responsibilities are with regard to handling credit cards.

Why do entire databases continue to get stolen?

Russo: All the information is contained in the logs so alerts are being set off to let you know something is going on, and if you're not looking at the logs on a regular basis somebody could be in there for weeks or even months stealing this data and you're not aware of it. There was a big merchant that got breached but they caught it immediately in their logs and they only lost four or five credit cards. So they did suffer a breach, but it was contained to only a few cards.

Is that the biggest problem? Ignoring the logs?

Russo: That's one of the things they're doing. In one case mentioned earlier if they were complaint there would have been no way for somebody to get in and get that data.

So it's a matter of failing to follow standard security policies?

Russo: Yes. They're not following basic security practices.

With the rise of credit card attacks being harvested via browsers, will PCI ever get into the business of certifying that the browser is secure? If you can certify what it takes to secure a Web site, why not the browser?

Russo: We're concerned about where credit card data is being collected and stored, not so much how you can get to see it. My browser does not need to be secure; the server holding the data does [for PCI compliance purposes].

If someone suspects a vendor is violating PCI requirements, how can that be reported?

Russo: Consumers can call the toll-free number on the back of their credit card.

What is your ultimate take-away message for readers?

Russo: Ultimately they need to make sure the merchants they're dealing with are PCI compliant. And

your credit card activity online. I can watch all my credit cards online to see what I'm spending, and what my wife and my kids are spending. You really should be monitoring your credit card statements."

--Bob Russo, general manager, PCI Security Standards Council

if you're a merchant you really have to be careful because consumers are getting smarter and smarter and if they find out you are not protecting their data, credit card data or personal data, they're going to walk away. And that's going to be the downfall of your business.

Tags: Security,

FEATURED VIDEO



ABOUT THE AUTHOR



Elinor Mills /   /

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. [E-mail Elinor](#). [See full bio](#)

/

YOU MAY ALSO LIKE



Teen shot dead after using app to track lost cell phone - CNET



See how that vertical 787 takeoff looked from the cockpit - CNET



How To Get Better Knees - Do This Daily

Instaflex Advanced
Sponsored



Millions of Shoppers Are Looking to Brad's Deals

BradsDeals.com
Sponsored

[Learn more](#)

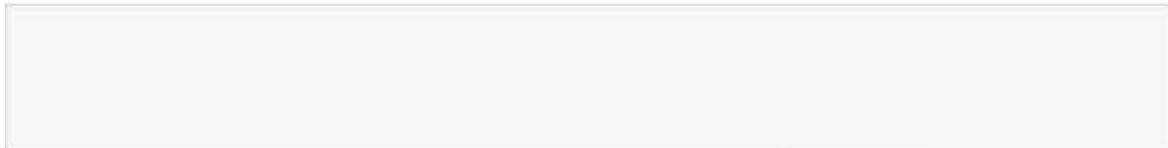
Powered by **YAHOO!** for you

DISCUSS PCI COMPLIANCE: WHAT IT IS AND WHY IT MATTERS...

4 Comments /

2 people following

[Log In](#)



✎ @ + Follow conversation

🔗 Share

Post Comment As...

SORT BY: [NEWEST](#) | [OLDEST](#) | [TOP COMMENTS](#)

[FAQs](#) / [Guidelines](#)

ToddBrandley

Nov 13, 2012

The best way to know for sure is is to check for a Trust Seal and click on it to make sure.. If it's a Trust Guard or McAfee seal the company has gone thru PCI scanning

← [REPLY](#) / [LIKE](#)

ToddBrandley

Nov 13, 2012

FTC-0002867

Trust Guard has been doing PCI scanning for years check out <http://www.trust-guard.com/?Click=b3144> for more information and solutions for your site.

← REPLY / 👍 LIKE

themhz

May 10, 2013

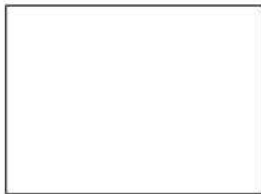
Excellent presentetion, thank you. One last question. Why would a merchant need to store credit card information on his-her database? can't just the bank do the work for the merchant?

← REPLY / 👍 LIKE

Show More Comments

Conversation powered by Livefyre

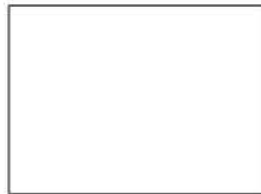
LATEST ARTICLES FROM CNET



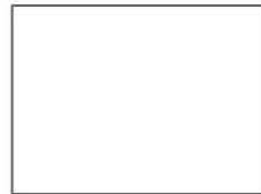
Get an official first look at 'Suicide Squad' in action



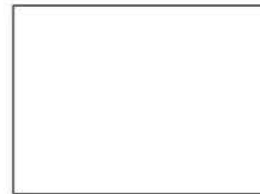
Pluto postage stamp on spacecraft heading for history July 14



The new Windows 10 notifications will follow you everywhere



As the Reddit Turns: Ex-CEO says Ellen Pao not to blame for firing of key exec



Gone in a flash? Facebook says Adobe's plug-in is a security risk no longer worth taking



REVIEWS

- All Reviews
- Audio
- Cameras
- Car Tech
- Desktops
- Laptops
- Phones
- Tablets
- TVs

NEWS

- All News
- Apple
- Crave
- Internet
- Microsoft
- Mobile
- Sci-Tech
- Security
- Tech Industry

VIDEO

- All Video
- Apple Byte
- CNET On Cars
- CNET Top 5
- CNET Update
- Next Big Thing
- The 404
- The Fix
- XCAR

MORE

- About CBS Interactive
- About CNET
- CNET 100
- CNET Deals
- CNET Forums
- CNET Magazine
- CNET Mobile
- Help Center
- Permissions

FOLLOW CNET VIA...

- Facebook
- Twitter
- Google+
- YouTube
- LinkedIn
- Tumblr
- Pinterest
- Newsletters
- RSS

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 51
TO EXPERT REPORT OF DR. ERIC B. COLE**

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

CONFIDENTIAL

From: Austin Appel [Austin.Appel@lifelock.com]
Sent: Monday, March 25, 2013 11:47 AM
To: David Bridgman
Subject: RE: Add (b) systems to (b)(3)61

Ok. These scans have been created and are currently scheduled to be run on April 4th.

Thanks,

Austin Appel
Information Security Analyst | LifeLock® - Relentlessly Protecting Your Identity™
O: 480.457.2061 | (b)(6),(b)(7)(C)
Austin.Appel@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: David Bridgman
Sent: Monday, March 25, 2013 11:23 AM
To: Austin Appel
Subject: Re: Add (b) systems to (b)(3)61

We are going to have to say YES. However, I'm not prepared to declare that to the Auditor. We need to scan and validate firewalls plus other controls.

David Bridgman, CISSP

Sr. Information Security Engineer | LifeLock® - Relentlessly Protecting Your Identity™

480.457.2029 Office | (b)(6),(b)(7)(C) Cell

David.Bridgman@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

LIFELOCK-0024609

CONFIDENTIAL

From: Austin Appel <Austin.Appel@lifelock.com>
Date: Monday, March 25, 2013 11:15 AM
To: David Bridgman <david.bridgman@lifelock.com>
Subject: RE: Add (b) systems to (b)(3):6(

OK. So, to be clear, those VLANs should be considered PCI VLANs now?

From: David Bridgman
Sent: Monday, March 25, 2013 11:13 AM
To: Austin Appel
Subject: Re: Add (b) systems to (b)(3):6(

It's for going forward. There is Credit card data stored on those systems. Let go ahead and create scans for each VLAN REDACTED This way we know what other hosts are on the network and can make sure they are all being patched in case one host get compromised within that VLAN.

David Bridgman, CISSP

Sr. Information Security Engineer | LifeLock® - Relentlessly Protecting Your Identity™

480.457.2029 Office | (b)(6),(b)(7) Cell
(C)

David.Bridgman@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: Austin Appel <Austin.Appel@lifelock.com>
Date: Monday, March 25, 2013 11:02 AM
To: David Bridgman <david.bridgman@lifelock.com>
Subject: RE: Add (b) systems to (b)(3):6(

Is this for a single scan or to be folded into the typical VRR process?

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

Thanks,

LIFELOCK-0024610

CONFIDENTIAL

Austin Appel

Information Security Analyst | LifeLock® - Relentlessly Protecting Your Identity™

O: 480.457.2061 | M: (b)(6),(b)(7)(C)

Austin.Appel@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: David Bridgman

Sent: Monday, March 25, 2013 10:51 AM

To: Austin Appel

Subject: Add (b) systems to (b)(3);6

Austin Please add the (b) systems to (b)(3);6 to scan.

REDACTED

David Bridgman, CISSP

Sr. Information Security Engineer | LifeLock® - Relentlessly Protecting Your Identity™

480.457.2029 Office | (b)(6),(b)(7)(C) Cell

David.Bridgman@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

LIFELOCK-0024611

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 52
TO EXPERT REPORT OF DR. ERIC B. COLE**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 53
TO EXPERT REPORT OF DR. ERIC B. COLE**



Date: 01/30/13

Security Department Goals 2013

- Update Lifelock's Security Posture and prioritize department activities by Q1 2013
- Update Security Department's Road map by Q1 2013
- Ensure the organization is PCI compliant by the end of Q2 2013
- Improve network forensics capabilities by implementing an enterprise network forensic system in Q2 2013.
- In-source (from Internal audit) third party management and user access reviews in Q2 2013
- Mature third party management program in Q2 2013
- (b)(3);6(f),(b)(4)
- Update and mature security incident procedures in Q2 2013; ensure the business understands the risk of the level of preparedness it chooses
- Mature compliance program to embed compliance into operational business activities by Q3 2013
- Improve employee awareness and education around email vulnerabilities by performing quarterly awareness tests beginning in Q3 2013.
- Perform high level assessment of business continuity plan in Q3 2013
- Update security documentation to reflect actual practices organization-wide by Q4 2013
- Develop high level security audit program in Q4 2013 to be implemented formally in 2014
- Improve monitoring of database logs by implementing an enterprise database logging solution by Q4 2013
- Improve operational efficiency by creating and maintaining procedures on log management, file integrity monitoring, intrusion prevention systems and desktop forensics systems by Q4 2013.
- Improve developer security education and awareness around coding in web and mobile based applications through training in 2013.
- Improve education in security threats and trends by attending security conferences and trainings in 2013.

David Bridgman Quarterly Goals

Q1

- Implement the network forensic system purchased in 2012 by the end of Q1.
- Conduct developer security training around mobile application on IOS, Android and Microsoft phones by the end of Q1.
- Create procedures for log management and file integrity monitoring by the end of Q1.
- Attend security-training conference by the end of Q1.

Q2

Information Security



- Ensure the organizations success in PCI compliance by the end of Q2.
- Conduct a PCI postmortem exercise by the end of Q2.
- Evaluate and select an enterprise database monitoring solution by the end of Q2.
- Conduct a security assessment and penetration test of the mobile application by the end of Q2.
- Create procedures for intrusion prevention systems by the end of Q2.

Q3

- Conduct and evaluation of the (b)(3):6(f),(b)(4) by the end of Q3.
- Evaluate and select a network access control solution replacement by the end of Q3.
- Conduct developer application security training by the end of Q3.
- Implement URL filtering within (b)(3):6(f) by the end of Q3.
- Create procedures for desktop forensics by the end of Q3.

Q4

- Conduct a penetration test of internal and external networks by the end of Q4.
- Conduct Employee security awareness training by the end of Q4.
- Implement an enterprise database monitoring solution by the end of Q4.

Austin Appel's Quarterly Goals

Q1

- (b)(3):6(f),(b)(4)
- Create a new system for malware analysis to provide better flexibility and capability than the old laptop solution
- (b)(3):6(f),(b)(4)

Q2

- Implement a process for scanning for open (improper permissions) Windows shares
- Conduct password assessment of (b)
- Develop user education and training program to augment email phishing assessments

Q3

- Create materials for application security training for developers
- (b)(3):6(f),(b)(4)
- Become fluent in the use of (b)(3):6(f),(b)(4)
- Attend security training conference(s)

Q4



- Implement a process for scanning shares (such as departmental_shares, etc.) for sensitive information
- Implement a solution for local workstation administrative accounts
- Investigate and test contactless credit card reading/cloning (useful for marketing/demos)

Anne-Marie Olson's Quarterly Goals

Q1

- Update Lifelock's Security Posture and prioritize department activities by Q1 2013
- Update Security Department's Road map by Q1 2013

Q2

- Ensure the organization is PCI compliant by the end of Q2 2013
- In-source (from Internal audit) third party management and user access reviews in Q2 2013
- Mature third party management program in Q2 2013

Q3

- Mature compliance program to embed compliance into operational business activities by Q3 2013
- Improve employee awareness and education around email vulnerabilities by performing quarterly awareness tests beginning in Q3 2013.
- Review and update content of security awareness training
- Attend CISM training September 2-9 in San Diego, CA (SecureNinja)

Q4

- Attend Annual ISSA International Conference in Nashville, TN October 8-10
- Test for CISM certification December 14
- Update security documentation to reflect actual practices organization-wide by Q4 2013
- Develop high level security audit program in Q4 2013 to be implemented formally in 2014

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

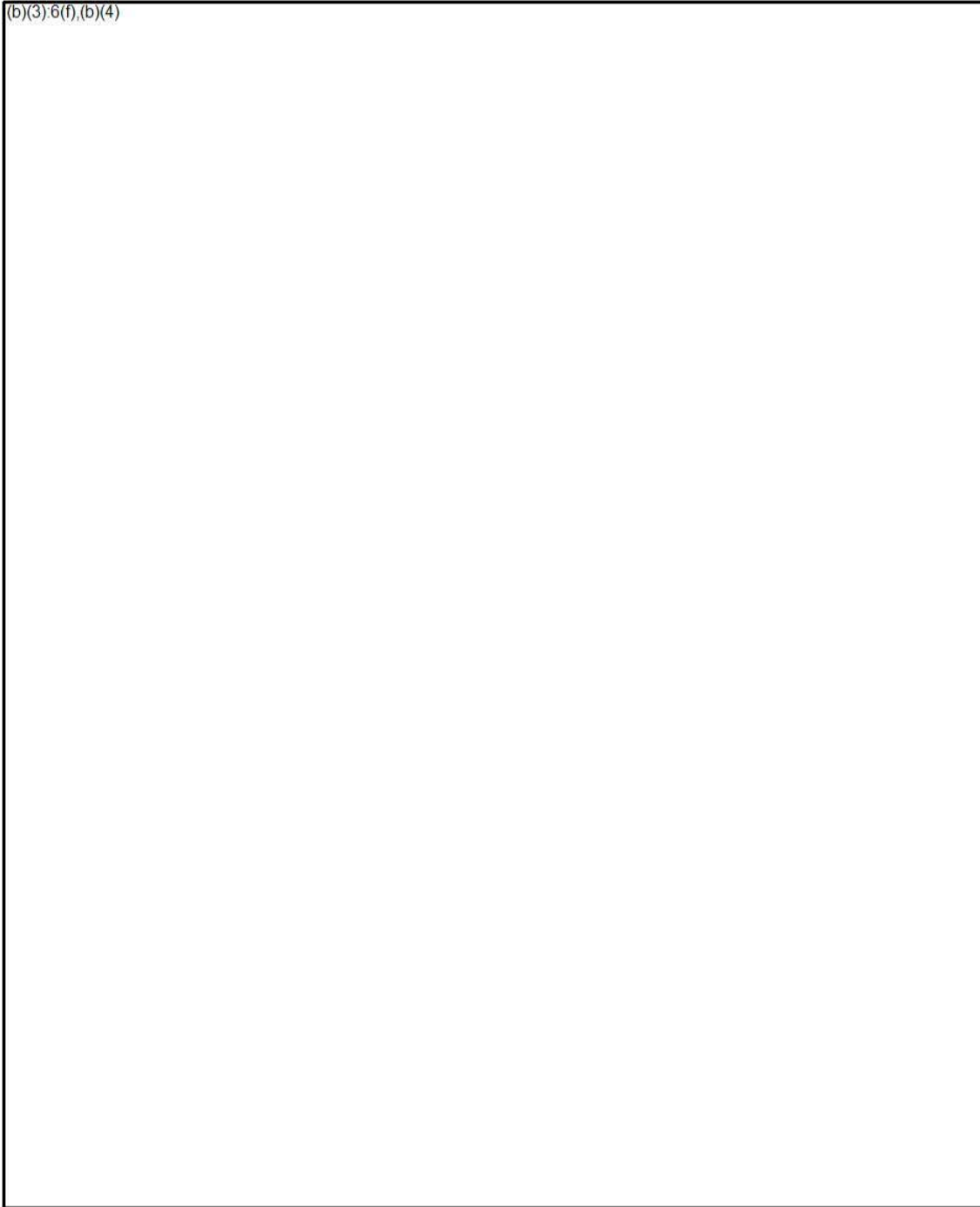
LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 54
TO EXPERT REPORT OF DR. ERIC B. COLE**


**2014 Enterprise Risk Assessment
Summary Report**

Submitted by Anne-Marie Olson
March 12, 2014

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



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



**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 55
TO EXPERT REPORT OF DR. ERIC B. COLE**

***This Attachment contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Attachment also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 56
TO EXPERT REPORT OF DR. ERIC B. COLE**

Adobe Security Bulletin

Security updates available for Adobe Flash Player

Release date: April 28, 2014

Vulnerability identifier: APSB14-13

Priority: [See table below](#)

CVE number: CVE-2014-0515

Platform: All Platforms

Summary

Adobe has released security updates for Adobe Flash Player 13.0.0.182 and earlier versions for Windows, Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh and Adobe Flash Player 11.2.202.350 and earlier versions for Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system.

Adobe is aware of reports that an exploit for CVE-2014-0515 exists in the wild, and is being used to target Flash Player users on the Windows platform. Adobe recommends users update their product installations to the latest versions:

- Users of Adobe Flash Player 13.0.0.182 and earlier versions for Windows should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 11.2.202.350 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.356.
- Adobe Flash Player 13.0.0.182 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 13.0.0.206 for Windows, Macintosh and Linux.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.0.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 11 will automatically be updated to the latest Internet Explorer 11 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.1.

Affected software versions

- Adobe Flash Player 13.0.0.182 and earlier versions for Windows
- Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh
- Adobe Flash Player 11.2.202.350 and earlier versions for Linux

To verify the version of Adobe Flash Player installed on your system, access the [About Flash Player page](#), or right-click on content running in Flash Player and select "About Adobe (or Macromedia) Flash Player" from the menu. If you use multiple browsers, perform the check for each browser you have installed on your system.

Solution

Adobe recommends users update their software installations by following the instructions below:

- Adobe recommends users of Adobe Flash Player 13.0.0.182 and earlier versions for Windows update to the newest version 13.0.0.206 by downloading it from the Adobe Flash Player Download Center, or via the update mechanism within the product when prompted.
- Adobe recommends users of Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh update to the newest version 13.0.0.206 by downloading it from the Adobe Flash Player Download Center, or via the update mechanism within the product when prompted.
- Adobe recommends users of Adobe Flash Player 11.2.202.350 and earlier versions for Linux update to Adobe Flash Player 11.2.202.356 by downloading it from the Adobe Flash Player Download Center.
- For users of Flash Player 11.7.700.275 and earlier versions for Windows and Macintosh, who cannot update to Flash Player 13.0.0.206, Adobe has made available the update Flash Player 11.7.700.279*, which can be downloaded [here](#).
- Adobe Flash Player 13.0.0.182 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 13.0.0.206 for Windows, Macintosh and Linux.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.0.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 11 will automatically be updated to the latest Internet Explorer 11 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.1.

* Beginning May 13, 2014, Adobe Flash Player 13 for Mac and Windows will replace version 11.7 as the extended support version. Adobe recommends users upgrade to version 13 to continue to receive security updates. See this blog post for further details <http://blogs.adobe.com/flashplayer/2014/03/upcoming-changes-to-flash-players-extended-support-release.html>

Priority and severity ratings

Adobe categorizes these updates with the following [priority ratings](#) and recommends users update their installation to the newest version:

Product	Updated version	Platform	Priority rating
Adobe Flash Player	13.0.0.206	Windows and Macintosh	1
	13.0.0.206	Internet Explorer 10 for Windows 8.0	1
	13.0.0.206	Internet Explorer 11 for Windows 8.1	1

13.0.0.206	Chrome for Windows, Macintosh and Linux	1
11.7.700.279	Windows and Macintosh	1
11.2.202.356	Linux	3

These updates address a [critical](#) vulnerability in the software.

Details

Adobe has released security updates for Adobe Flash Player 13.0.0.182 and earlier versions for Windows, 13.0.0.201 and earlier versions for Macintosh and Adobe Flash Player 11.2.202.350 and earlier versions for Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system. Adobe recommends users update their product installations to the latest versions:

- Users of Adobe Flash Player 13.0.0.182 and earlier versions for Windows should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 11.2.202.350 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.356.
- Adobe Flash Player 13.0.0.182 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 13.0.0.206 for Windows, Macintosh and Linux.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.0.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 11 will automatically be updated to the latest Internet Explorer 11 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.1.

These updates resolve a buffer overflow vulnerability that could result in arbitrary code execution (CVE-2014-0515).

Affected Software	Recommended Player Update	Availability
Flash Player 13.0.0.182 and earlier versions for Windows	13.0.0.206	Flash Player Download Center
Flash Player 13.0.0.201 and earlier versions for Macintosh	13.0.0.206	Flash Player Download Center
Flash Player 13.0.0.182 and earlier versions for Windows (network distribution)	13.0.0.206	Flash Player Licensing
Flash Player 13.0.0.201 and earlier versions for Macintosh (network distribution)	13.0.0.206	Flash Player Licensing
Flash Player 11.2.202.350 and earlier for Linux	11.2.202.356	Flash Player Download Center
	13.0.0.206	Google Chrome Releases

Flash Player 13.0.0.182 and earlier for Chrome (Windows, Macintosh and Linux)		
Flash Player 13.0.0.182 and earlier in Internet Explorer 10 for Windows 8.0	13.0.0.206	Microsoft Security Advisory
Flash Player 13.0.0.182 and earlier in Internet Explorer 11 for Windows 8.1	13.0.0.206	Microsoft Security Advisory

Acknowledgments

Adobe would like to thank Alexander Polyakov of [Kaspersky Labs](#) for reporting [CVE-2014-0515](#) and for working with Adobe to help protect our customers.

 [Choose your region](#) [Products](#) [Downloads](#) [Learn & Support](#) [Company](#)

Copyright © 2015 Adobe Systems Incorporated. All rights reserved.
[Terms of Use](#) | [Privacy](#) | [Cookies](#)
[AdChoices](#)

Severity ratings

Priority and Severity rating systems for Security Bulletins

The Adobe Priority Rating System is a guideline to help our customers in managed environments prioritize Adobe security updates. We base our priority rankings on historical attack patterns for the relevant product, the type of vulnerability, the platform(s) affected, and any potential mitigations that are in place.

The definitions of the priority ratings are:

Rating	Definition
Priority 1	This update resolves vulnerabilities being targeted, or which have a higher risk of being targeted, by exploit(s) in the wild for a given product version and platform. Adobe recommends administrators install the update as soon as possible. (for example, within 72 hours).
Priority 2	This update resolves vulnerabilities in a product that has historically been at elevated risk. There are currently no known exploits. Based on previous experience, we do not anticipate exploits are imminent. As a best practice, Adobe recommends administrators install the update soon (for example, within 30 days).
Priority 3	This update resolves vulnerabilities in a product that has historically not been a target for attackers. Adobe recommends administrators install the update at their discretion.

The Adobe Severity Rating System is a guideline to help our developers assess the security impact of known software vulnerabilities.

The definitions of the severity ratings are:

Rating	Definition
Critical	A vulnerability, which, if exploited would allow malicious native-code to execute, potentially without a user being aware.
Important	A vulnerability, which, if exploited would compromise data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer.
Moderate	A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit.

Low

A vulnerability that has minimal impact and is extremely difficult to exploit.

[SECURITY BULLETINS](#)
[NOTIFICATION SERVICE](#)
[ALERT US](#)
[SEVERITY RATINGS](#)
[ACKNOWLEDGMENTS](#)
[PSIRT PGP Key](#)



Choose your region [Products](#) [Downloads](#) [Learn & Support](#) [Company](#)

Copyright © 2015 Adobe Systems Incorporated. All rights reserved.
[Terms of Use](#) | [Privacy](#) | [Cookies](#)
[AdChoices](#)

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED ATTACHMENT 57
TO EXPERT REPORT OF DR. ERIC B. COLE**

Trojan.Cryptowall

Risk Level 1: Very Low

Summary

Technical Details

Removal

Printer Friendly Page

Discovered: June 19, 2014**Updated:** March 3, 2015 12:41:26 PM**Type:** Trojan**Systems Affected:** Windows 2000, Windows 7, Windows 95, Windows 98, Windows Me, Windows NT, Windows Vista, Windows XP

Trojan.Cryptowall is a Trojan horse that encrypts files on the compromised computer. It then asks the user to pay to have the files decrypted.

The threat typically arrives on the affected computer through spam emails, exploit kits hosted through malicious ads or compromised sites, or other malware.

Once the Trojan is executed on the compromised computer, it creates a number of registry entries to store the path of the encrypted files and run every time the computer restarts. It encrypts files with particular extensions on the computer and creates additional files with instructions on how to obtain the decryption key.

This threat family attempts to convince the user to pay money in order to get the key to unlock their files. It uses a variety of different techniques in order to encourage the user to pay the ransom.

Note: Trojan Cryptodefense is a variant of Trojan.Cryptowall.

Infection

The Trojan is mainly distributed through spam campaigns, compromised websites, malicious ads, or other malware.

In Cryptowall spam campaigns, the emails usually contain a malicious attachment and include a message attempting to convince the user to download the file. The email could claim that the attachment is an invoice, an undelivered package notice, or an incoming fax report. If the user opens the attachment, then their computer will be infected with Trojan.Cryptowall.

The Trojan may also be distributed through exploit kits hosted on compromised websites or malicious ads. Some of the exploit kits that have been used to compromise users' computers with the threat include the Rig exploit kit and the Nuclear exploit kit. Symantec has extensive IPS protections in place against these kits.

The Trojan may also arrive through other threats that have already compromised the computer, such as Downloader.Upatre or Trojan.Zbot.

Functionality

The Trojan was designed to prevent the user from accessing their files and force them to pay the attacker in order to regain access. It does this by encrypting a wide variety of files on the compromised computer using public/private key encryption with a strong 2048-bit RSA key.

Once the files are encrypted, the Trojan displays a text document or HTML page with a message. The message informs the user that their files have been encrypted and gives instructions on how to obtain the decryption key needed to unlock the files. It may also warn users that the decryption key will be deleted after a certain time period to pressure the user into paying sooner. The attacker may demand hundreds of US dollars in payment and the amount may increase after a specified time period.

Search Threats

Search by name

Example:

W32.Beagle.AG@mm



STAR Malware Protection Technologies

The security technologies Symantec creates

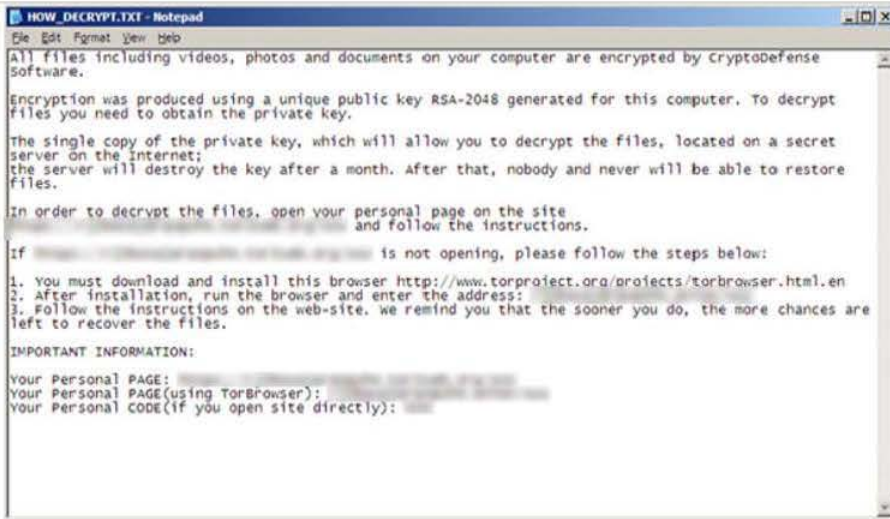
Learn more

ISTR20

2015 Internet Security Threat Report, Vol 20

Symantec data and analysis on the 2014 threat landscape

Get the report



The message also contains a link to a website where the user can make the payment. These sites are typically hosted on the anonymous Tor network, which helps the attacker hide their identity. The threat may ask the user to download a Tor network browser in order to view the site, though newer versions of the threat do not require the user to do this. The user may have to pay using cryptocurrencies such as bitcoin to further prevent the attacker's identity from being traced.

Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is not made before **02/04/14 - 09:03** the cost of decrypting files will increase 2 times and will be **1000 USD/EUR**.

Your system: Windows XP (x32) First connect IP: [redacted]

Refresh
Payment
FAQ
My screen
Test decrypt

We present a special software - CryptoDefense Decrypter - which allow to decrypt and return control to all your encrypted files.

How to buy CryptoDefense decrypter?



1. You should register Bitcoin wallet ([click here for more information with pictures](#))
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

 - [redacted] - This fantastic service allows you to search for people in your community willing to sell bitcoins to you directly.
 - [redacted] - An international directory of bitcoin exchanges.
 - [redacted] - Recommended for fast, simple service.
 - [redacted] - Bitcoin exchange based in the United States. (Highly rated).
 - [redacted] - A multi currency bitcoin exchange based in Slovenia. (Highly rated).
 - [redacted] allows direct bitcoin purchases on their site. They're based in Australia but serve an international clientele.
3. Send 1.09 BTC to Bitcoin address: [redacted] [Get QR code](#)
4. Enter the Transaction ID and select amount:

1.09 BTC ≈ 500 USD
Clear

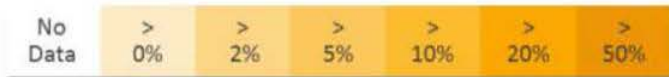
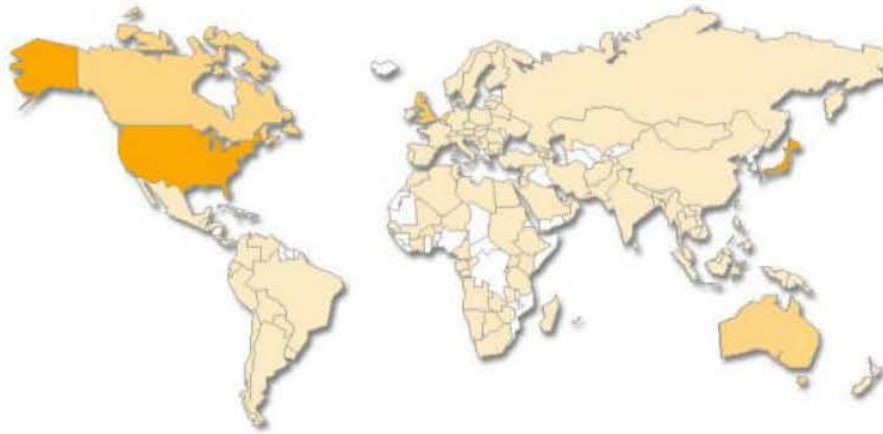
Note: Transaction ID - you can find in detailed info about transaction you made.
5. Please check the payment information and click "PAY".

PAY

Even if the user pays the ransom, there's no guarantee that the attacker will provide the decryption key needed to unlock their files.

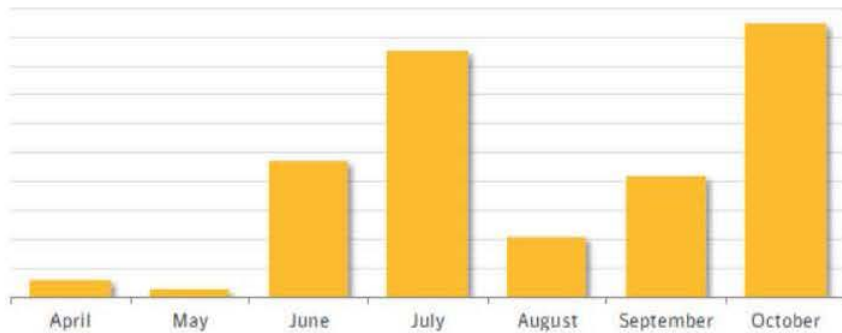
Geographical distribution

Symantec has observed the following geographic distribution of this threat:



Prevalence

Symantec has observed the following global infection trends between April and October 2014:



Symantec protection

The following Symantec detections protect against this threat family.

AV

- Trojan.Cryptodefense
- Trojan.Cryptdeflgen1
- Trojan.Cryptdeflgen2
- Trojan.Cryptdeflgen3
- Trojan.Cryptdeflgen4
- Trojan.Cryptdeflgen8
- Trojan.Cryptdeflgen9
- Trojan.Cryptdeflgen10
- Trojan.Cryptdeflgm

IPS

- System Infected: Trojan.Cryptodefense Activity

Heuristic detections

- WS.Trojan.H
- SONAR.Heuristic.112
- SONAR.Heuristic.113
- SONAR.Cryptodefense!g1

Reputation detections

- Suspicious.Cloud.2
- Suspicious.Cloud.5.A
- Suspicious.Cloud.5.D

Antivirus Protection Dates

- **Initial Rapid Release version** June 19, 2014 revision 034
- **Latest Rapid Release version** June 5, 2015 revision 039
- **Initial Daily Certified version** June 20, 2014 revision 002

- **Latest Daily Certified version** June 6, 2015 revision 001
- **Initial Weekly Certified release date** June 25, 2014

Click [here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

Writeup By: Laura O'Brien, Jeet Morparia

Summary | [Technical Details](#) | [Removal](#)



UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __3__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Exhibit also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __5__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

April 7, 2015

Susan Pope, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Ms. Pope:

This completes our response to your request letter dated March 13, 2015, supplementing our responses dated March 31, 2015. We have set forth the requested information as set forth in your letter. (Please note that your questions are set forth below in bold typeface).

SPECIFICATIONS

1. With respect to the “Internet” acquisition channels identified in Annex 2 of your March 11, 2015 response, you identified five (5) separate Internet channel subcategories (affiliate, paid search, display, email, and mobile app enrollments). For the relevant period,

d. For each of the five (5) Internet channel subcategories, identify the top five (5) advertisements or promotional materials disseminated by LifeLock, or on behalf of LifeLock, by both: (i) dissemination, and (ii) enrollment revenues, for each month.

Please see the requested information set forth in Annex 1.

e. Provide enrollment and revenue information for each top 5 advertisement or promotional material, identified in 1.d., above.

Please see the requested information set forth in Annex 1.

2. With respect to the “TV” acquisition channel, for the relevant period, to the extent not previously provided,

a. Identify the top 3 TV advertisements aired by LifeLock, or on behalf of LifeLock, by both: (i) dissemination, and (ii) enrollment revenues, for each

month, and provide for each, the Date, Time, Station, Show, Title and Market identifying when and where these advertisements were run.

Please see the requested information set forth in Annex 2.

b. Provide enrollment and revenue information for each advertisement, identified in 2.a., above.

Please see the requested information set forth in Annex 2.

3. With respect to the “Radio” acquisition channel, for the relevant period, to the extent not previously provided,

a. Please describe any Radio acquisition channel subcategories LifeLock uses to maintain enrollment and/or revenue information, if any.

Radio can be grouped into three categories: A-List, which is top national radio personalities; Non A-List, which is lower-performing radio personalities and other radio assets such as drive time radio; and Testing, which is comprised of new shows, markets and formats that LifeLock is testing.

b. Identify the top 5 Radio advertisements (broken down by each subcategory referenced in response to 3.a., above, if any) aired by LifeLock, or on behalf of LifeLock, by both: (i) dissemination, and (ii) enrollment revenues, for each month, and provide for each, the Date, Time, Station, Show, Title and Market identifying when and where these advertisements were aired.

Please see the requested information set forth in Annex 3.

c. Provide enrollment and revenue information for each top 5 Radio advertisements, identified in 3.b., above.

Please see the requested information set forth in Annex 3.

4. With respect to the “Direct Mail” acquisition channel, for the relevant period, to the extent not previously provided,

a. Identify the top 5 Direct Mail advertisements disseminated by LifeLock, or on behalf of LifeLock, by both: (i) dissemination, and (ii) enrollment revenues, for each month.

Please see the requested information set forth in Annex 4.

- b. Provide enrollment and revenue information for each Top 5 Direct Mail advertisement, identified in 4.a., above.**

Please see the requested information set forth in Annex 4.

- 5. With respect to the “Other Marketing Promotions” acquisition channel, for the relevant time period, to the extent not previously provided,**

- c. Identify the top 5 Other Marketing Promotion advertisements or materials disseminated by LifeLock, or on behalf of LifeLock, by both: (i) dissemination, and (ii) enrollment revenues, for each month.**

Please see the requested information set forth in Annex 5.

- d. Provide enrollment and revenue information for each top 5 Other Marketing Promotion advertisement, identified in 5.c., above.**

Please see the requested information set forth in Annex 5.

- 7. To the extent not previously provided, provide a copy of all advertisements or promotional materials identified by LifeLock in response to questions 1 through 6, above.**

These materials are being produced on a CD which is being separately delivered to you.

Please advise whether you have any questions regarding the foregoing; please accord the foregoing information confidential treatment under the Commission’s Rules of Practice.

Very truly yours,

A handwritten signature in blue ink that reads "Andrew Berg" with "H.B." written below it.

Andrew G. Berg
Counsel to LifeLock, Inc.

cc: Gregory Madden, Esq.

FTC has submitted 'Ex. 5 - LIFELOCK-0135515 (TV Air Dates).xlsx' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __14__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

“2013 RA” worksheet

LIFELOCK INC.
RISK ASSESSMENT DETAIL

TYPE	SOURCE	RISK	Risk Metrics					Overall Risk Score
			Name	Likelihood	Impact	Velocity	Complexity	
			REF	Weight	(0.1, 0.1, 0.2, 0.4)			
STRAT	Governance	(b)(3)-(b)(7), (b)(4)						
	Planning & Allocation							
	Major Initiatives							
	Brand & Communication							
OPER	Sales & Marketing							
	Member Services							
	Purchasing & Supply							
	People/Human Resources							
	Fulfillment							
	Assets							
COMP	Conduct							
	Legal							
	Regulatory							
FINL	Liquidity							
	Accounting & Reporting							
	Tax							
	Capital							
	Market							
	Internal Control Over Finl Reporting							
IT	IT Governance							
	IT Structure							
	Architecture							
	Proj Management/SDLC							
	Enterprise Security							
	Applications/Databases							
	Operations							
	Support							
	Disaster Recovery							
	Infrastructure							

- 0.25 Likelihood
- 0.25 Impact
- 0.10 Velocity
- 0.15 Complexity
- 0.25 Control Maturity
- 1.00

- 1 Risk is low as existing controls in place and have been documented, tested
- 2 Risk is medium as existing controls are in place but not formally documented or tested
- 3 Risk is high as controls are not consistently followed or are not in place
- 4 Risk is very high as existing controls have failed previously or are not documented

**“Sorted 2013 RA”
worksheet**

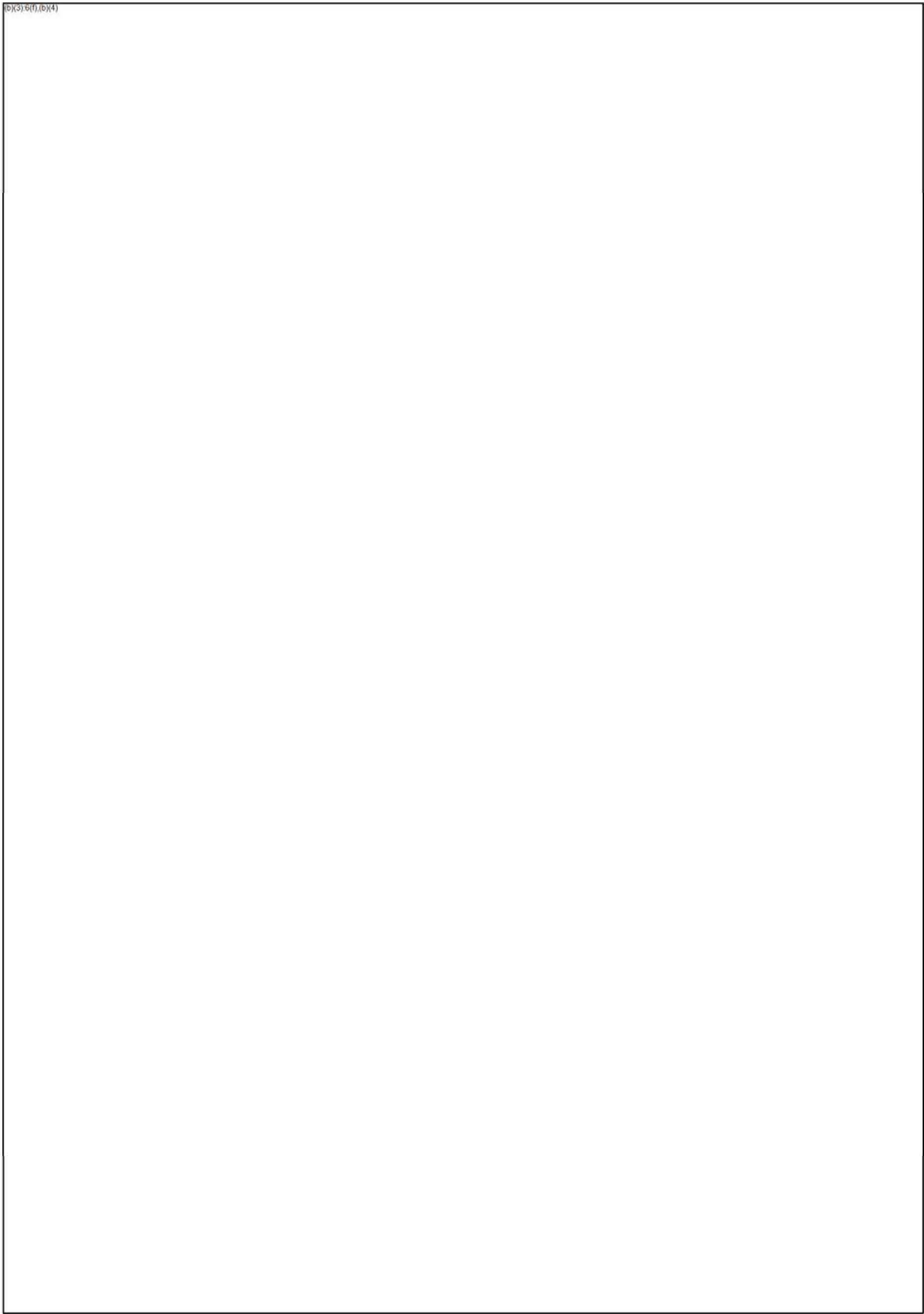
LIFELOCK INC.
RISK ASSESSMENT OVERVIEW

Auditable Risks			Risk Metrics						Overall Risk Score
TYPE	SOURCE	RISK	REF	Name Weight	Likelihood	Impact	Velocity	Complexity	
IT	Enterprise Security	(b)(3),(6),(b)(4)							
COMP	Regulatory								
FINL	Internal Control Over Finl Reporting								
IT	Architecture								
IT	Applications/Databases								
IT	Infrastructure								
IT	Disaster Recovery								
STRAT	Major Initiatives								
COMP	Legal								
FINL	Accounting & Reporting								
OPER	Sales & Marketing								
FINL	Tax								
IT	Proj Management/SDLC								
IT	Operations								
STRAT	Governance								
STRAT	Planning & Allocation								
OPER	Member Services								
STRAT	Brand & Communication								
OPER	Purchasing & Supply								
IT	IT Governance								
IT	IT Structure								
IT	Support								
OPER	People/Human Resources								
COMP	Conduct								
FINL	Liquidity								
FINL	Capital								
FINL	Market								
OPER	Assets								

- 0.25 Likelihood
- 0.25 Impact
- 0.10 Velocity
- 0.15 Complexity
- 0.25 Control Maturity
- 1.00

- 1 Risk is low as existing controls in place and have been documented, tested
- 2 Risk is medium as existing controls are in place but not formally documented or tested
- 3 Risk is high as controls are not consistently followed or are not in place
- 4 Risk is very high as existing controls have failed previously or are not documented

“Instructions” worksheet



**“Type 2011 rev”
worksheet**

Risk ID #	Information Asset Type	Risk	Threat	Vulnerability	Security Concern	ISO 27001	PI	FTC	Probability	Impact	Financial	Legal/Regulatory	Member Loyalty	Initial Risk	Chance of detection	Risk Priority Number	Risk Rating	Controls	Residual Risk Rating	Notes/References	
					I = Integrity A = Avail				L = 0.1 M = 0.5 H = 1.0	L = 10 M = 50 H = 100				Prob X Imp L = 0.10 M = 25.50 H = 100	Very easy = 1 Effort needed = 2 Low likelihood = 4 Very difficult = 5	Risk X L = 0 - 49 M = 50 - 199 H = 200 - 500		Controls in place to mitigate risk	Final risk rating after controls		
1	Information (Member Data)				C, I	X	X	X			X	X	X								
2	Information (Member Data)				I	X	X	X			X	X	X								
3	Information (Member Data)				CIA	X	X	X			X	X	X								
4	Information (Member Data)				A	X	X	X			X	X	X								
5	Information (Member Data)				CIA	X	X	X			X	X	X								
6	Information (Member Data)				A	X	X	X			X	X	X								
7	Information (Member Data)	LOSS, THEFT OR DISCLOSURE OF MEMBER SENSITIVE DATA			A	X	X	X			X	X	X								
8	Information (Member Data)				A	X	X	X			X	X	X								
9	Information (Member Data)				A	X	X	X			X	X	X								
10	Information (Member Data)				C	X	X	X			X	X	X								
11	Information (Member Data)				C	X	X	X			X	X	X								
12	Information (Member Data)				C, I	X	X	X			X	X	X								
13	Information (Member Data)				C, I	X	X	X			X	X	X								
14	Hardware				IA	X	X	X			X	X	X								
15	Hardware				CIA	X	X	X			X	X	X								
16	Hardware				CIA	X	X	X			X	X	X								
17	Hardware				IA	X	X	X			X	X	X								
18	Hardware				IA	X	X	X			X	X	X								
19	Hardware	HARDWARE UNAVAILABILITY			A	X	X	X			X	X	X								
20	Hardware				A	X	X	X			X	X	X								
21	Hardware				A	X	X	X			X	X	X								
22	Hardware				IA	X	X	X			X	X	X								
23	Hardware				IA	X	X	X			X	X	X								
24	Hardware				A	X	X	X			X	X	X								
25	Hardware				A	X	X	X			X	X	X								
26	Software				I	X	X	X			X	X	X								
27	Software				I	X	X	X			X	X	X								
28	Software				A	X	X	X			X	X	X								
29	Software				C	X	X	X			X	X	X								
30	Software				C	X	X	X			X	X	X								
31	Software	SOFTWARE FUNCTIONALITY PERFORMANCE			I	X	X	X			X	X	X								
32	Software				I	X	X	X			X	X	X								

Risk ID #	Information Asset Type	Risk	Threat	Vulnerability	Security Concern I = Integrity A = Avail	ISO 27001	PI	FTC	Probability L = 0.1 M = 0.5 H = 1.0	Impact L = 10 M = 50 H = 100	Financial Operations	Risk Areas Legal/Regulatory Member Loyalty	Initial Risk Prob X Imp L = 0.10 M = 25.50 H = 100	Chance of detection Very easy = 1 Effort needed = 2 Low likelihood = 4 Very difficult = 5	Risk Priority Number Risk X Chance of Detection	Risk Rating L = 0 - 49 M = 50-199 H = 200 - 500	Controls	Residual Risk Rating	Notes/References
33	Software				C, A	X	X	X			X	X	X						
34	Software				C, A	X	X	X			X	X	X						
35	Software				A	X					X	X	X						
36	Software				A	X	X	X			X	X	X						
37	Software				A	X	X	X			X	X	X						
38	Physical Assets				A	X					X	X	X						
39	Physical Assets				I, A	X	X	X			X	X	X						
40	Physical Assets				I, A	X	X	X			X	X	X						
41	Physical Assets				I, A	X	X	X			X	X	X						
42	Physical Assets				I, A	X	X	X			X	X	X						
43	Physical Assets				I, A	X	X	X			X	X	X						
44	Physical Assets	LOSE, THEFT OR DISCLOSURE OF PHYSICAL ASSETS			A	X					X	X	X						
45	Physical Assets				A	X					X	X	X						
46	Physical Assets				A	X					X	X	X						
47	Physical Assets				I	X					X	X	X						
48	Physical Assets				C, A	X	X	X			X	X	X						
49	Physical Assets				C, A	X	X	X			X	X	X						
50	Physical Assets				A	X					X	X	X						
51	Physical Assets				A	X	X	X			X	X	X						
52	Physical Assets				A	X					X	X	X						
53	People				I	X					X								
54	People				I	X					X	X	X						
55	People				C	X	X	X			X	X	X						
56	People				C	X	X	X			X	X	X						
57	People				C	X	X	X			X	X	X						
58	People				A	X					X	X	X						
59	People				A	X					X	X	X						
60	People				I	X					X	X	X						
61	People				I	X	X	X			X	X	X						
62	People				I	X	X	X			X	X	X						
63	People				A	X					X	X	X						
64	Services				A	X	X	X			X	X	X						
65	Services				I	X	X	X			X	X	X						
66	Services				I	X	X	X			X	X	X						
67	Services				I	X	X	X			X	X	X						
68	Services				I	X					X	X	X						
69	Services				I	X	X	X			X	X	X						
70	Services				C	X	X	X			X	X	X						
71	Services	INSECURE UNAUTHORIZED OR IMPROPER SERVICES			I, A	X	X	X			X	X	X						
72	Services				I, A	X	X	X			X	X	X						
73	Services				I, A	X	X	X			X	X	X						

Risk ID #	Information Asset Type	Risk	Threat	Vulnerability	Security Concern I = Integrity A = Avail	ISO 27001	PCI	FTC	Probability L = 0.1 M = 0.5 H = 1.0	Impact L = 10 M = 50 H = 100	Risk Areas			Initial Risk Prob X Imp L = 0.10 M = 25.0 H = 100	Chance of detection Very easy = 1 Effort needed = 2 Low likelihood = 4 Very difficult = 5	Risk Priority Number Risk X Change of Direction	Risk Rating L = 0 - 49 M = 50 - 199 H = 200 - 500	Controls	Residual Risk Rating	Notes/ References
											Financial	Operations	Legal/Regulatory							
74	Services				I.A	X	X	X												
75	Services				I.A	X	X	X												
76	Services				I.A	X	X	X												
77	Services				I.A	X	X	X												
78	Services				I.A	X	X	X												
79	Services				C	X	X	X												

NOTE FOR 2011 REVIEW AND UPDATE

IN REVIEWING AND UPDATING 2011 RISK ASSESSMENT WORKBOOK, THE EXISTING WORKBOOK FROM 2010 WAS SELECTED AS THE STARTING POINT. THIS WAS PER BELOW. THE DATA AND SYSTEMS FOR EMPLOYEE AND COMPANY DATA.

A TOTAL OF 33 SUCH RISKS WERE IDENTIFIED AND REMOVED FROM THE 2010 LISTING. BOTH THE DIA AND INFO SEC MANAGER INDEPENDENTLY PROVIDED INPUT FOR IMPACT PROBABILITY AND DETECTION. CALCULATED SCORES WERE COMPARED AND EDITED TO ARRIVE AT THE FINAL SCORES ABOVE.

TV

**“Sorted RPN 2011
rev” worksheet**

Risk ID #	Information Asset Type (Information, Hardware, Assets, People, Services)	Threat	Vulnerability	Source	Security Concern (C = Confidentiality, A = Availability)	SOX Computing Controls (PCI, FTC)	Probability (L = 0.1, M = 0.5, H = 1.0)	Impact (L = 10, M = 25, H = 100)	Risk Areas (Financial, Operations, Regulatory, Legal)	Initial Risk (Prob X Imp L = 0-10, M = 25, H = 100)	Chance of detection (Very easy = 1, Relatively easy = 2, Moderate = 3, Low likelihood = 4, Very difficult = 5)	Risk Priority Number (Risk X Chance of Detection)	Risk Rating (L = 0 - 49, M = 50 - 99, H = 200 - 500)	Risk Disposition	Action Plan	Due Date
1	Information (Member Data)				C, I	X X X X										12/21/2012
2	Hardware				C, L, A	X X X X										12/21/2012
3	Software				C, L, A	X X X X										12/21/2012
4	Services				C, L, A	X X X X										12/21/2012
5	People				C, L, A	X X X X										12/21/2012
6	Hardware				C, L, A	X X X X										12/21/2012
7	Software				C, L, A	X X X X										12/21/2012
8	Services				C, L, A	X X X X										12/21/2012
9	People				C, L, A	X X X X										12/21/2012
10	Information (Member Data)				C, I	X X X X										12/21/2012
11	Information (Member Data)				C, I	X X X X										12/21/2012
12	Information (Member Data)				C, I	X X X X										12/21/2012
13	Information (Member Data)				C, I	X X X X										12/21/2012
14	Information (Member Data)				C, I	X X X X										12/21/2012
15	Information (Member Data)				C, I	X X X X										12/21/2012
16	Information (Member Data)				C, I	X X X X										12/21/2012
17	Information (Member Data)				C, I	X X X X										12/21/2012
18	Information (Member Data)				C, I	X X X X										12/21/2012
19	Hardware				A	X X X X										12/21/2012
20	Hardware				A	X X X X										12/21/2012
21	Hardware				A	X X X X										12/21/2012
22	Hardware				A	X X X X										12/21/2012
23	Hardware				A	X X X X										12/21/2012
24	Software				A	X X X X										12/21/2012
25	Software				A	X X X X										12/21/2012
26	Software				A	X X X X										12/21/2012
27	Software				A	X X X X										12/21/2012
28	Physical Assets				A	X X X X										12/21/2012
29	Software				C	X X X X										12/21/2012
30	Software				C	X X X X										12/21/2012
31	Software				C	X X X X										12/21/2012
32	Software				C	X X X X										12/21/2012
33	Software				C	X X X X										12/21/2012
34	Physical Assets				C	X X X X										12/21/2012

Risk ID #	Information Asset Type	Threat	Vulnerability	Source	Security Concern C = Conf I = Integrity A = Avail	SOX - General Computing Controls	PCI	FTC	Probability L: = 0.1 M: = 0.5 H: = 1.0	Impact L = 10 M = 50 H = 100	Risk Areas Financial Operations Legal Regulatory	Initial Risk Prob X Imp L = 0.10 M = 25, 50 H = 100	Chance of detection Very easy = 1 Relatively easy = 2 Effort needed = 3 Low likelihood = 4 Very difficult = 5	Risk Priority Number Risk X Chance of Detection	Risk Rating L: = 0 - 49 M: = 50-199 H: = 200 - 500	Risk Disposition	Action Plan	Due Date
29	42	Physical Assets			IA		X	X	X									
30	43	Physical Assets			IA		X	X	X									
31	47	Physical Assets			I		X											
32	53	People			I													
33	54	People			I		X											
34	64	Services			A		X	X	X									
35	65	Services			I		X	X	X									
36	66	Services			I		X											
37	70	Services			C		X	X	X									
38	71	Services			IA		X	X	X									
39	72	Services			IA		X	X	X									
40	73	Services			IA		X	X	X									
41	74	Services			IA		X	X	X									
42	75	Services			IA		X	X	X									
43	76	Services			IA		X	X	X									
44	77	Services			IA		X	X	X									
45	78	Services			IA		X	X	X									
46	79	Services			C		X											
47	36	Physical Assets			A		X											
48	3	Information (Member Data)			CIA		X	X	X									
49	4	Information (Member Data)			A		X	X	X									
50	5	Information (Member Data)			CIA		X	X	X									
51	14	Hardware			IA		X	X	X									
52	28	Software			A		X	X	X									
53	34	Software			C, A		X	X	X									
54	36	Software			A		X	X	X									
55	37	Software			A		X	X	X									
56	39	Physical Assets			IA		X	X	X									
57	44	Physical Assets			A		X											
58	46	Physical Assets			A		X											
59	2	Information (Member Data)			I		X	X	X									
60	15	Hardware			CIA		X	X	X									
61	16	Hardware			CIA		X	X	X									
62	17	Hardware			IA		X	X	X									
63	35	Software			A		X											
64	55	People			C		X	X	X									
65	61	People			I		X	X	X									
66	69	Services			I		X	X	X									
67	33	Software			C, A		X	X	X									
68	45	Physical Assets			A		X											
69	49	Physical Assets			C, A		X	X	X									
70	50	Physical Assets			A		X											
71	51	Physical Assets			A		X	X	X									
72	52	Physical Assets			A		X											
73	60	People			I		X											
74	13	Information (Member Data)			C, I		X	X	X									
75	21	Hardware			A		X	X	X									
76	48	Physical Assets			C, A		X	X	X									
77	31	Software			I		X	X	X									
78	58	People			A		X											
79	59	People			A		X											

**“High RPN 2011 rev”
worksheet**

Risk ID #	Information Asset Type	Threat	Vulnerability	Security Concern	ISO 27001	PCI	FTC	Probability L: = 0.1 M: = 0.5 H: = 1.0	Impact L = 10 M = 50 H = 100	Risk Areas				Initial Risk Prob X Imp L = 0-10 M = 25,50 H = 100	Chance of detection Very easy = 1 Relatively easy = 2 Effort needed = 3 Low likelihood = 4 Very difficult = 5	Risk Priority Number Risk X Chance of Detection	Risk Rating L: = 0 - 49 M: = 50-199 H: = 200 - 500	
										Financial	Operations	Legal Regulatory	Member Loyalty					
1	1	Information (Member Data)	[Redacted]	C, I	x	x	x	[Redacted]	[Redacted]	x	x	x	x	[Redacted]	[Redacted]	[Redacted]		
2	41	Physical Assets		I A	x	x	x			x	x	x	x				x	x
3	56	People		C	x	x	x			x	x	x	x				x	x
4	66	Services		I	x	x	x			x	x	x	x				x	x
5	67	Services		I	x	x	x			x	x	x	x				x	x
6	24	Hardware		A	x	x	x			x	x	x	x				x	x
7	25	Hardware		A	x	x	x			x	x	x	x				x	x
8	57	People		C	x	x	x			x	x	x	x				x	x
9	10	Information (Member Data)		C	x	x	x			x	x	x	x				x	x
10	11	Information (Member Data)		C	x	x	x			x	x	x	x				x	x
11	12	Information (Member Data)		C I	x	x	x			x	x	x	x				x	x
12	62	People		I	x	x	x			x	x	x	x				x	x
13	63	People		A	x	x	x			x	x	x	x				x	x

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

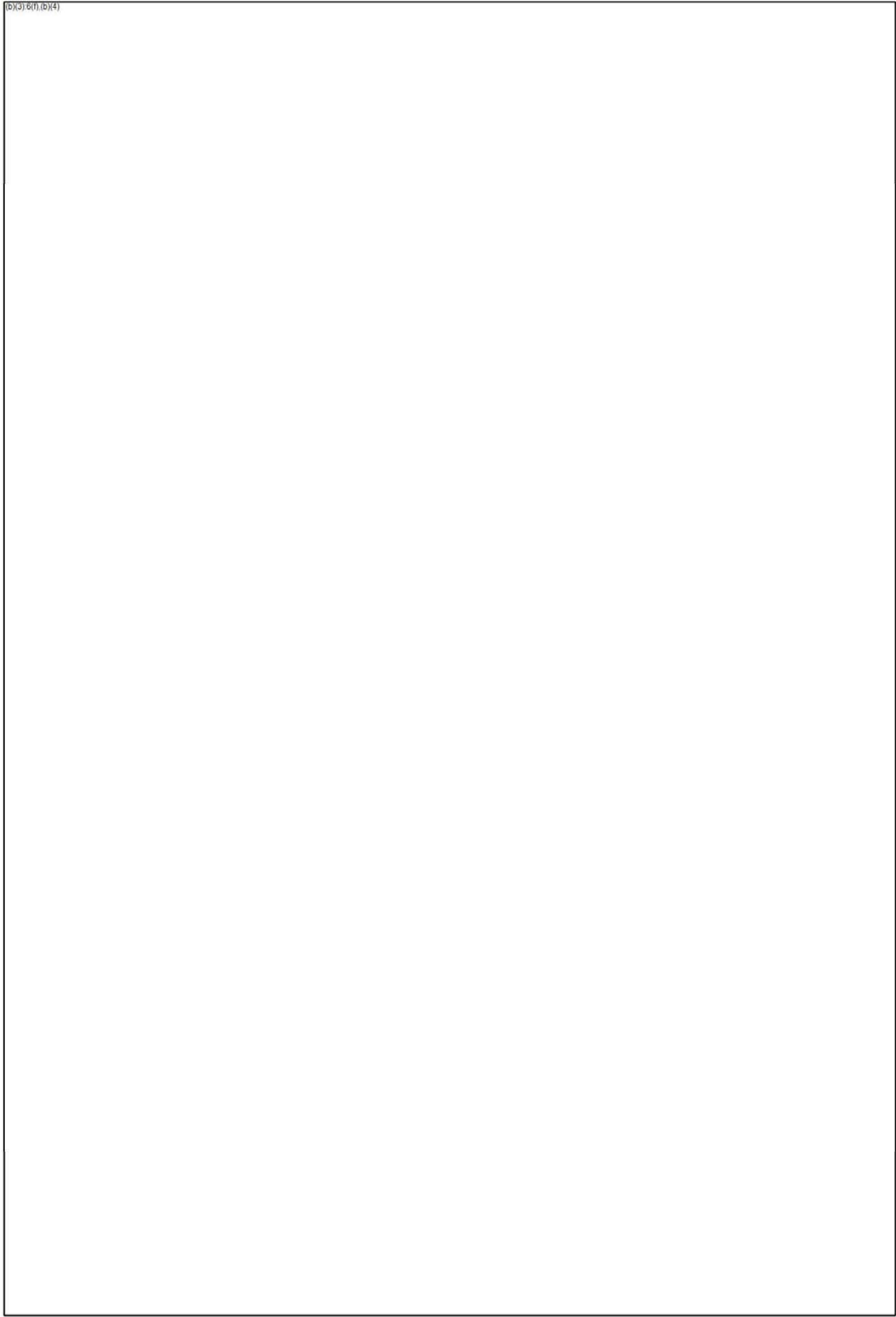
**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __15__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

“Instructions” worksheet

(b)(3) & (b)(4)



**“RA Type 2012”
worksheet**

Risk ID	Mission Area	Threat	Vulnerability	Source	Security Controls	FTC	Probability	Impact	Risk Areas			Initial Risk	Chance of Detection/Prevention	Risk Priority Number	Risk Rating	Controls	Residual Risk Rating	Notes/References
									Financial	Operational	Legal/Regulatory							
17	Information Security Physical Security Access Control Business Continuity	Threat Threat	Vulnerability Vulnerability	Source Source	Security Controls C-500 Integrity A-1000 A-1000	FTC FTC SOX SOX	Probability L = 0.1 M = 0.5 H = 1.0	Impact L = 10 M = 50 H = 100	Financial Operational Legal/Regulatory	Risk X Imp L = 10 M = 25 H = 100	Very easy = 1 Easy = 2 Low likelihood = 4 Very difficult = 5	Risk X Chance of Detection	L = 0.45 M = 50/100 H = 200 - 500	Controls Controls to mitigate/reduce risk	Residual Risk Rating Final risk rating after controls	Notes/References Notes/References		
18	Services	Services	Services	Services	C, L, A													

**“Sorted RPN 2012”
worksheet**

**“HIGH RPN 2012”
worksheet**

Risk ID #	Information Asset Type	Threat	Vulnerability	Source	Security Concern	SOX	PCI	FTC	Probability	Impact	Risk Areas	Initial Risk	Chance of detection	Risk Priority Number	Risk Rating	Controls	Residual Risk Rating	Risk Disposition	Action Plan	Due Date	Notes/Reference
1	Information (Member Data)				C = Conf I = Integrity A = Avail	X X X X			L = 0.1 M = 0.5 H = 1.0	L = 10 M = 50 H = 100	Financial Operations Legal/Regulatory Member Loyalty	Prob X Imp L = 0.10 M = 25.50 H = 100	Very easy = 1 Easy = 2 Effort needed = 3 Low likelihood = 4 Very difficult = 5	Risk X Chance of Detection	L = 0 - 40 M = 50 - 199 H = 200 - 500	Controls to mitigate/reduce risk	Final risk rating after controls		Initial approved Action Plan (review as plan further develops)		
2	Software				C.I.A.	X X X					X										
3	Services				C.I.A.	X X X					X										
4	Services				A	X X X					X										
5	People				C.I.A.	X X X					X										
6	Information (Member Data)				C.I.	X X X X					X X X X										

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __16__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

***This Exhibit contains excerpted pages only and does not contain all of the
pages in the full bates range of the original document.**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __17__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

***This Exhibit contains excerpted pages only and does not contain all of the
pages in the full bates range of the original document.**

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

December 24, 2014

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

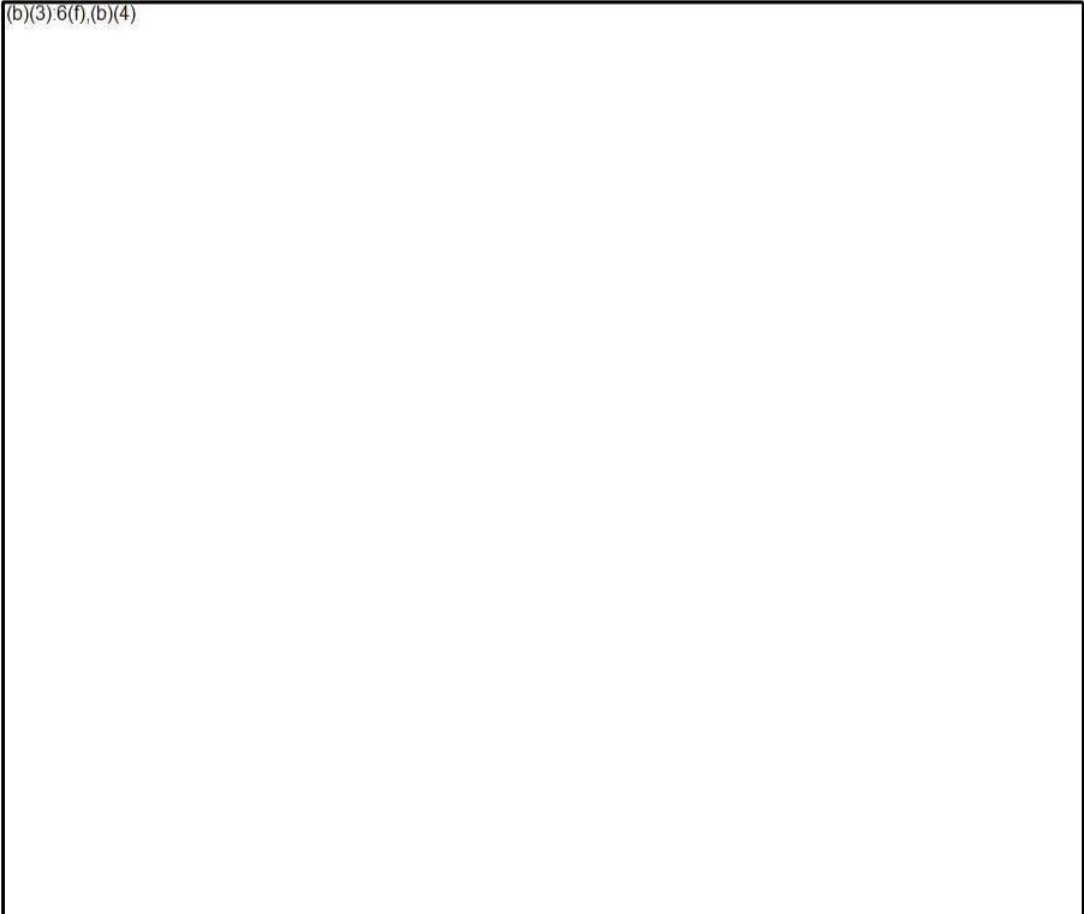
Dear Mr. Madden:

This responds to your letter dated December 12, 2014 in which you made follow-up inquiries to our December 9th submission relating to LifeLock's information and data security compliance. We have set forth the requested information following the order of the questions in your letter. (Please note that your questions are set forth below in bold typeface).

- 1. Describe fully and in detail the purpose(s) for, and content of, a "Member Services remediation case file," and include in your description an identification of any and all personal information that is included in any such file.**

(b)(3);6(f);(b)(4)

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



- 2. Explain what the term "inactive" means and identify in your explanation how many such files were affected, how many of the affected files were for individuals who were LifeLock members at the time of the attack, and how many of the affected files were for individuals that were former LifeLock members at the time of the attack.**

The term "inactive" as used in our December 9th response refers to a closed or completed remediation case of a LifeLock member who alleged that they had experienced identity theft. In the database affected by the referenced ransomware attack there were a total of 254 remediation case files (described above) and 54 other (non-remediation related) files affected. The other non-remediation related files consisted of Specialist and Member Services Agent resources, such as call scripts, outbound call tracking sheets, and team performance metrics. Outbound tracking sheets may have contained some Personal Information that included member name, phone number, and email address. Of the 254 remediation case files affected there are only 7 cases that were still active or open at the time of the occurrence of the ransomware attack (all of the others were closed and inactive).

- At the time of the ransomware attack:
 - 251 members out of the 254 remediation case files were current members

- 3 members out of the 254 remediation case files had cancelled their LifeLock service before the occurrence of the ransomware attack
- After the time of the ransomware attack:
 - 7 members out of the 254 remediation case files have cancelled their LifeLock service (these cancellations were not related to or as a consequence of the ransomware attack but were non-renewals for other reasons or cancellations for non-payment of membership fees – the cancellations had occurred prior to LifeLock and the members becoming aware of the ransomware attack)

3. Describe fully and in detail all other information affected by the attack.

As stated above, 54 of the affected files were not remediation case files. Given that the files were encrypted as a result of the ransomware attack and are therefore inaccessible, LifeLock is unable to precisely document the data in these files; however, these resource files typically include resources such as call scripts, outbound call tracking sheets, and team performance metrics. Outbound tracking sheets typically contain member name, phone number, and email address; while they may contain member identification they do not contain member SSN or DOB data. Call scripts are used for outbound campaigns for various purposes, such as a “welcome to LifeLock” message or advisory of new service. Outbound call tracking sheets are used to track agent work, whether or not a member has been reached, a message left, inability to contact, and notes on the interaction with the member. Team performance metrics are folders created at the discretion of the agent team to track performance against internal KPIs such as average handling time for calls, conversions per day (to membership), upgrade statistics, quality performance surveys and results.

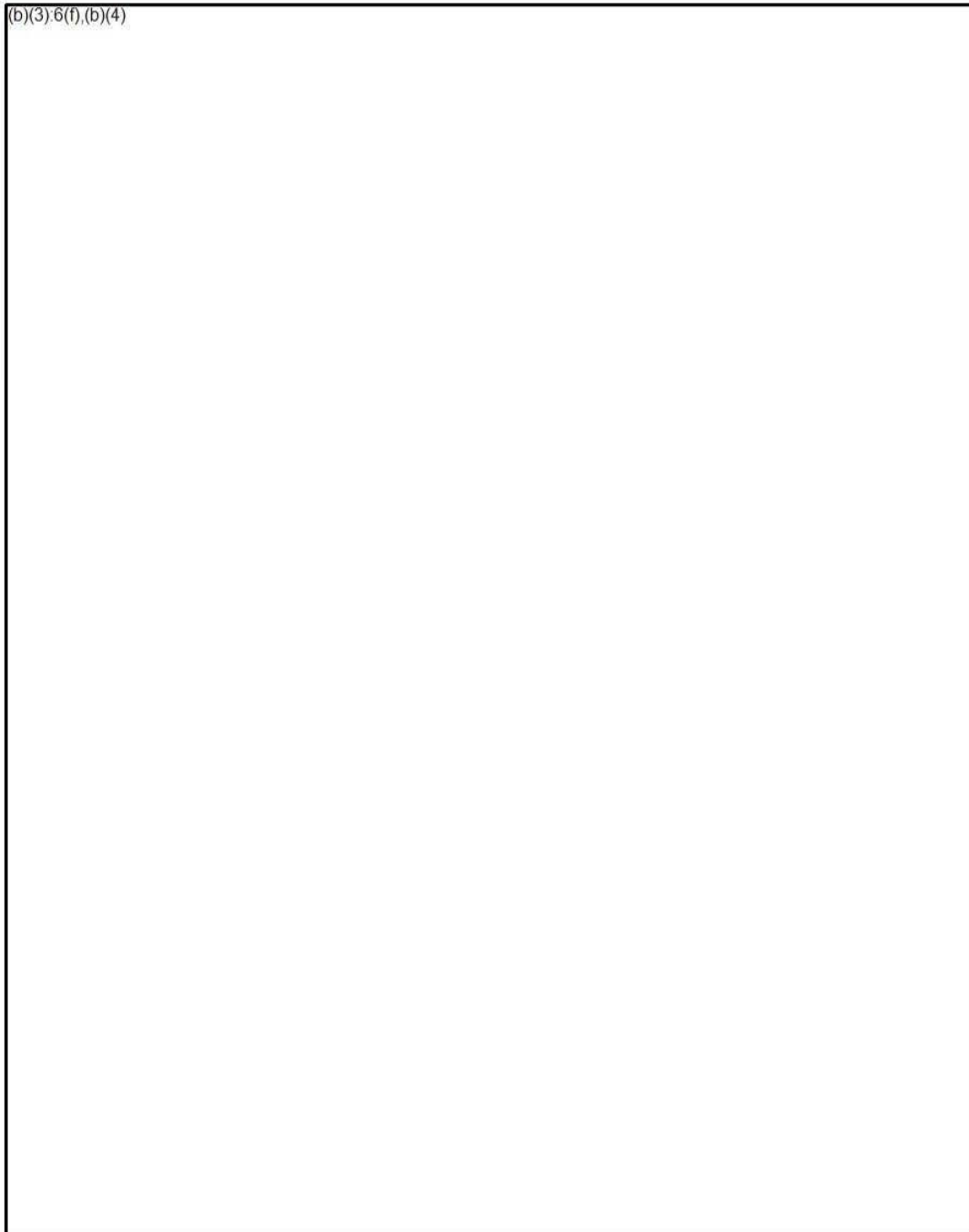
4. Identify and describe all files with any member's personal information that were affected by the ransomware attack and include in your description an identification of any and all personal information that is included in any such file.

As noted in response to Question 3 above, 54 files were non-remediation related internal document files used by Specialists and Member Services Agents to track various performance-related information. (Please refer to our response to Question 3 for a description of the content of those files.) The remainder of the files affected (254 in number) were remediation case files (which are described in response to Question 1 above).

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

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

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



- 5. Identify the number of LifeLock members whose personal information was affected by the ransomware attack. Identify how many of these members were LifeLock members at the time of the attack, and how many were not LifeLock members at the time of the attack.**

Please see the response to Question 2 above.

- 6. For any individuals affected by the ransomware attack that were not LifeLock members at the time of the attack, identify the personal information that LifeLock had for such members, and explain the basis for LifeLock's retention of that personal information.**

Please see our response to Question 1 above for details pertaining to the Personal Information that LifeLock may have retained for former members that had closed remediation files in the database at the time of the ransomware attack. As a result of the encryption used by the attack (LifeLock is unable to access those files, as stated in our December 9th letter) we are unable to confirm the specific Personal Information contained in each member file but they may have included any or all of the data described above in the response to Question 1.

- 7. Provide a description of how the ransomware attack impacts LifeLock's ability to provide its alert service. Include in your description an explanation of how LifeLock provides its alert service to LifeLock members affected by the ransomware attack.**

The ransomware attack did not and does not impact, in any manner, LifeLock's ability to provide its alert service to its members; LifeLock's alert services are provided through an entirely separate platform/system. As stated previously in our December 9th letter, the ransomware attack only affected the resolution database by making certain limited files and data inaccessible to LifeLock.

- 8. Describe how the ransomware attack impacts LifeLock's ability to provide any other services that LifeLock provides its members.**

The ransomware attack potentially impacts only 7 LifeLock members with current "open" active remediation cases, and even then in only a very limited manner. In the event that one of the documents contained in the affected remediation case files is needed to provide continued assistance in the resolution of a member's identity theft, LifeLock would need to obtain another copy of that document from the specific member. LifeLock expects that, as needed, all such documents should be readily obtainable from the member as the member was the original source of these documents and in most cases these documents would have been sent electronically by the member (via PDF or fax) to LifeLock. With the very limited exception of these case remediations for these 7 members only, the ransomware attack does not impact LifeLock's ability to provide any other services to its members.

- 9. Produce all versions of notifications provided to current or former LifeLock members. Describe how the notifications were provided, and identify the number of members that received each such notification. Include in your response an**

We want to assure you that the security of your information has been maintained and, we apologize for any inconvenience this may cause. Thank you for your LifeLock membership, we look forward to continue helping you live freely in an always-connected world.

10. Identify the total revenue that LifeLock received from affected members during the time that their membership services were affected.

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



Please advise whether you have any questions regarding the foregoing; please accord the foregoing information confidential treatment under the Commission's Rules of Practice.

Very truly yours,



Andrew G. Berg
Counsel to LifeLock, Inc.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __18__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

December 9, 2014

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This supplements our December 3, 2014 response to your letter dated November 18, 2014 in which you made follow-up inquires (as modified in your December 4th email to me) to our previous submissions relating to LifeLock's information and data security practices. We have set forth the requested supplemental information below, which supplements our response appearing on page 5 of our December 3rd response; your supplemental request is set forth below in bold typeface.

Identify all LifeLock employee and member information that (b)(3):6(f), (b)(4) was able to access, and all employee and member information (b)(3):6(f), (b)(4) would have been able to access, at that time. Include in your response data that is input or known by LifeLock as part of its use into databases that were accessible through this attack scenario and identify any metadata that is associated with these databases including whether any fields are encrypted within the database. For employee information, identify the roles and privileges, including any administrative rights, that were accessible.

Identify all privileges and capabilities that were or could be obtained by the attacker such as the ability to modify objects of the domain (e.g., add/remove software, modify/disable security mechanisms, add/modify accounts) including the ability to interact with other domains or components of LifeLock's network that are beyond the initial attack domain. Identify each department that has objects within the domain(s) that could be compromised by an attacker. In addition, please provide the Metranet data dictionary.

(b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4) Domain Admin access to a domain in Active Directory gives a user "superuser" access to a domain and is the highest level of access that a user can have. (b)(3):6(f),(b)(4)
(b)(3):6(f),(b)(4)

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

Separately, LifeLock also wanted to notify you of a recent ransomware attack that it experienced. The incident, which occurred in late September 2014 and was reportedly also experienced by several hundred companies, was directed at companies running an older version of Adobe Flash. LifeLock was running an older version of Adobe Flash on its (b)(3):6(f),(b)(4) servers which were awaiting updated versions of that software. LifeLock's deployment of the updated Adobe Flash version (which was to be automatic) was delayed due to deployment issues attributable to (b)(3):6(f),(b)(4) product. The ransomware in question infected LifeLock's (b)(3):6(f),(b)(4) and (b)(3):6(f),(b)(4) drives along with one LifeLock Member Services employee's local drive. (b)(3):6(f),(b)(4) LifeLock's information security consultant that was retained to assess the attack, confirmed that no PII of any type was exfiltrated or either viewed or accessed by any unauthorized individuals. The ransomware simply resulted in certain member information (mostly relating to inactive Member Services remediation case files) being encrypted and therefore unavailable to LifeLock without access to the ransom "key" (LifeLock did not pay the ransom that was demanded). Although not required by applicable law, LifeLock has notified all of the impacted members of the incident and has requested their assistance in restoring member information.

Please advise whether you have any questions regarding the foregoing, and accord the foregoing information confidential treatment under the Commission's Rules of Practice.

Very truly yours,



Andrew G. Berg
Counsel to LifeLock, Inc.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __19__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Exhibit also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

January 2, 2015

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This responds to your letter dated December 16, 2014 in which you made follow-up inquiries to our December 9th submission relating to LifeLock's information and data security compliance. We have set forth the requested information following the order of the questions in your letter. (Please note that your questions are set forth in bold typeface.)

- 1. Identify the specific "ransomware" that was used in the attack on LifeLock. Include in your response any identifying characteristics or information regarding the ransomware used in the attack on LifeLock.**

The specific ransomware used in the LifeLock attack was "Cryptowall". Identifying characteristics of Cryptowall include the ransom message/decryption instructions; network traffic to known addresses associated with this wave of Cryptowall attacks; and the presence of artifacts on the file system of the affected system consistent with a Cryptowall payload execution.

- 2. Describe all known capabilities of the ransomware, including but not limited to whether it read LifeLock data and or made changes to LifeLock data. Include in your description how the encryption occurred.**

The Cryptowall ransomware targets Windows operating systems. Once executed, Cryptowall searches for files that match a number of file extensions commonly associated with documents and other files likely to contain information necessary to conduct business on the affected system as well as any network file shares that are mapped on the system. It then reaches out to Command and Control (C2) servers to get a unique encryption **REDACTED** key in order to encrypt the files on the affected system. It uses this key to encrypt (with a secure **REDACTED** bit encryption) the files matching its filters and for which it has read/write permissions. The Cryptowall ransomware has no other known capabilities.

Notably, it has not been found to perform data exfiltration nor install other malware that has this capability.

- 3. Provide the exact dates and times: (a) the ransomware attack began; (b) the attack was detected by LifeLock; and (c) LifeLock halted the attack. Include in your description the duration of the attack.**

The attack began on September 23, 2014 at 12:37 p.m. when (b)(3):6(f),(b)(4) (who is a LifeLock Resolution Specialist I, Member Services) browsed to a website that contained a malicious ad redirect. Within this same minute, the malware was downloaded and unpacked into memory in the process of execution. The attack was detected by LifeLock on November 4th at approximately 8:48 a.m.

Due to the nature of the configuration for the LifeLock (b)(3):6(f),(b)(4) systems, the attack was halted the afternoon (at 4:36 p.m.) of September 23rd when (b)(3):6(f),(b)(4) logged off of her session on the (b)(3):6(f),(b)(4) system. (The use of (b)(3):6(f),(b)(4) by LifeLock's Member Services agents is described in more detail in response to Questions 7 and 8 below.) The attack was halted at that time because upon logoff, the local temp files for each terminal session are deleted. The Cryptowall ransomware was not able to install itself onto (b)(3):6(f),(b)(4) file system or to obtain persistence through the Windows Registry.

- 4. Describe in detail how LifeLock identified and resolved the ransomware attack. Your description should include, at a minimum, how the attack was discovered (e.g., automated monitoring tool(s), specific alert(s)), each person who was told of the attack, each person who took action as a result of the attack, all actions taken in response to the attack, and an identification of all documents related or referring to the attack or LifeLock's response to the attack.**

The following series of events describe in detail how LifeLock discovered, identified, addressed and resolved the Cryptowall ransomware attack.

On Monday, November 3, 2014 at 8:16 a.m., a (b)(3):6(f),(b)(4) ticket (REDACTED 3) was created by (b)(3):6(f),(b)(4) (LifeLock Resolution Specialist II, Member Services) regarding the inability to open a document. The service ticket was initially assigned to the (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) group in accordance with standard process at ticket generation. (b)(3):6(f),(b)(4) then routes the ticket request based on the content of the service ticket.

On Tuesday, November 4, 2014, at 8:43 a.m., (b)(3):6(f),(b)(4) assigned the service ticket to the (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) group because the issue initially appeared to be a file permissions issue (which the (b)(3):6(f),(b)(4) group controls). At 9:15 a.m., (b)(3):6(f),(b)(4) (Operations Analyst II, Information Security team) was assigned the service ticket by (b)(3):6(f),(b)(4) (Info Sec Ops Technician) when it appeared that a permissions issue might not be the source of the

(<http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Agent-AJBH/detailed-analysis.aspx>) had been reviewed which provided more information about the command-and-control used by one variant of the Cryptowall malware (all the command-and-control traffic was found to be communicating with a single Citrix REDACTED machine). The team also discussed next steps, which included restoring the environment and retaining a third party to continue to search for the source of the infection (because at that point the LifeLock internal team had nearly exhausted their resources).

(b)(3):6(f),(b)(4) then had a subsequent discussion wherein they agreed that (b)(3):6(f),(b)(4) would retain (b)(3):6(f),(b)(4) to do a more in-depth review and to provide expert advice on Cryptowall. (b)(3):6(f),(b)(4) was contacted and a SOW was created for (b)(3):6(f),(b)(4) retention. (b)(3):6(f),(b)(4) investigation is described in detail in LifeLock's response to Question 21, below.)

- 5. Provide the basis for the statement that this attack was experienced by several hundred companies and identify those companies that LifeLock knows experienced this attack.**

Dell SecureWorks published a Threat Analysis on CryptoWall, (located at <http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/>) where they state that "Between mid-March and August 24, 2014, nearly 625,000 systems were infected with CryptoWall." Additionally, another article (<http://www.networkworld.com/article/2688993/security/malvertising-campaign-delivers-digitally-signed-cryptowall-ransomware.html>) discusses the same "wave" of infections of an undiscovered variant of CryptoWall that LifeLock was affected by. This conclusion was also generally confirmed by (b)(3):6(f),(b)(4) in its forensic investigation of the attack.

- 6. Identify the Adobe Flash version that LifeLock was running on each (b)(3):6(f),(b)(4) server at the time of the ransomware attack.**

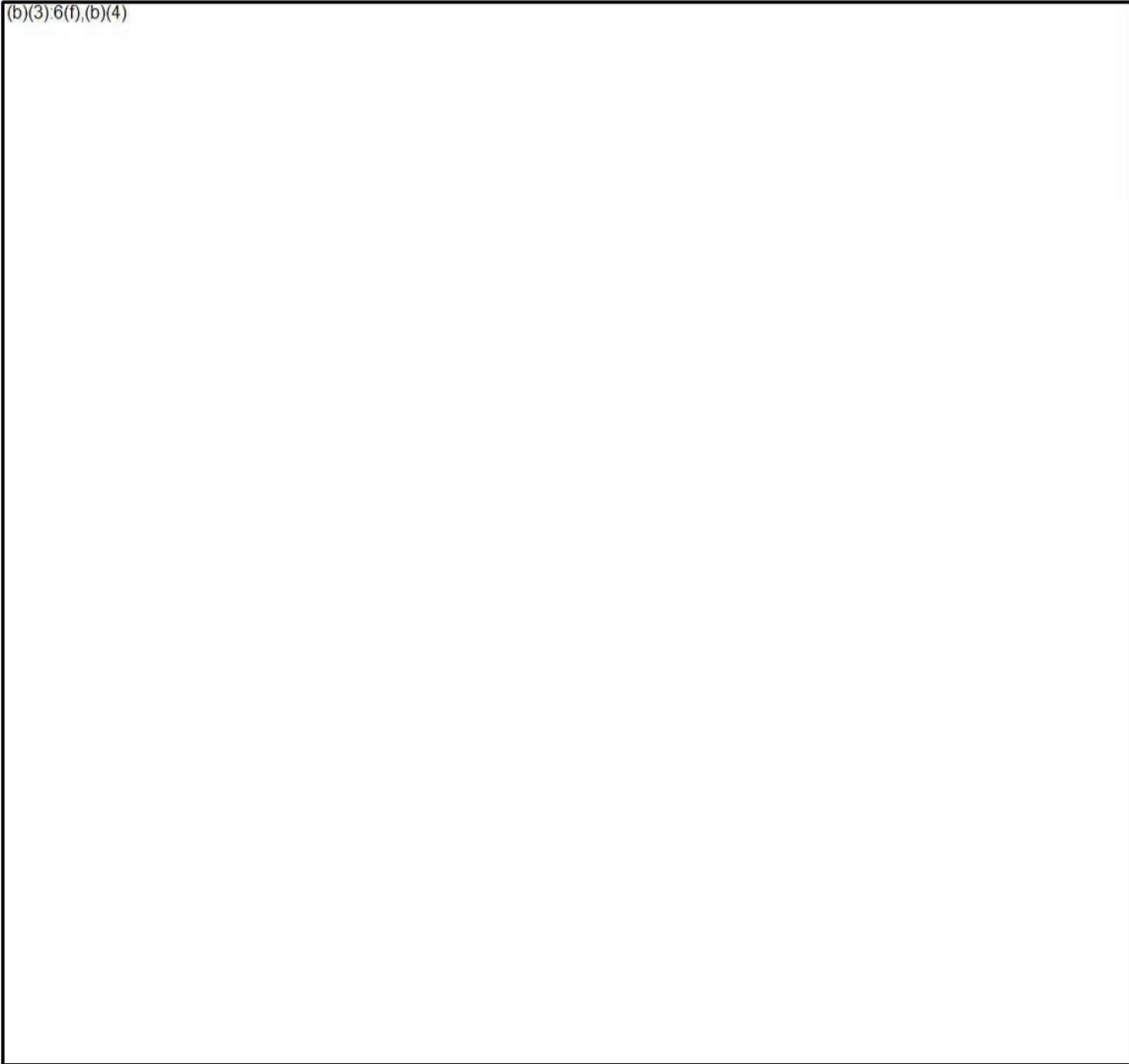
Each (b)(3):6(f),(b)(4) server was running Adobe Flash Player 12.0.0.4 at the time of the attack.

- 7. Specifically identify and describe fully the purpose(s) of each (b)(3):6(f),(b)(4) server that was running an older version of Adobe Flash at the time of the ransomware attack. Identify any personal information held on each such server at that time.**

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

8. For each identified (b)(3):6
(b)(4) server, describe all of the server's functions, all data that it processes, through either storage or remote access (including mapped network drives), and its position in LifeLock's computing environment, including other network(s) and system(s) to which it is attached.

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



9. Specifically identify the Microsoft SCCM product that is referenced in your response, including the version of the Microsoft SCCM product.

System Center Configuration Manager 2007 R3.

10. Describe in detail the deployment issues that delayed the update of Adobe Flash.

LifeLock utilizes (b)(3):6(f),(b)(4) and (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) to deploy software and patches to its endpoints. (b)(3):6(f),(b)(4) is used to manage patches, deploy software, and to inventory LifeLock's windows software/hardware. (b)(3):6(f),(b)(4) is used to manage the distribution of updates to computers on LifeLock's network. Both products are from (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) supplies a (b)(3):6(f),(b)(4) catalog in order to simplify the deployment and management of Adobe Flash. (b)(3):6(f),(b)(4) is a tool used with (b)(3):6(f),(b)(4) to increase the efficiency in installing, updating and patching software.

The specific issue that LifeLock encountered that caused the deployment issues is that the (b)(3):6(f),(b)(4) received an internal application error and refused to publish updates to the (b)(3):6(f),(b)(4) server. LifeLock's (b)(3):6(f),(b)(4) team could see the updates in (b)(3):6(f),(b)(4) but the actual contents of the patch were not able to be uploaded. Since the UTS team was unable to resolve the error, the UTS teams contacted Microsoft seeking assistance with a resolution of the issue. UTS then manually created (b)(3):6(f),(b)(4) packages (instead of relying on the (b)(3):6(f),(b)(4) catalog supplied by (b)(3):6(f),(b)(4) to push the updates to Adobe Flash. These packages were tested and used to update Adobe Flash on the referenced (b)(3):6(f),(b)(4) on November 12, 2014.

11. Identify how long the update of Adobe Flash had been delayed, state whether the decision to delay the update was documented, identify each person involved in the decision to delay the update, and identify all documents relating or referring to that decision.

The following table identifies the sequence of events that occurred in connection with the updating of Adobe Flash. Notably, there was no formal decision or documentation to delay the update; the delay was an ongoing condition caused by the technical issues encountered during the deployment of the updates.

Date	Event
9/11/14	(b)(3):6(f),(b)(4) identified that we were not running the current version of Adobe Flash and discussed the issue with (b)(3):6(f),(b)(4). Once confirmed, Adobe Flash was scheduled to be updated.
10/6/14	(b)(3):6(f),(b)(4) started the work to apply updates to Adobe Flash.
10/9/14	(b)(3):6(f),(b)(4) discovered an issue preventing Adobe Updates from working normally with (b)(3):6(f),(b)(4) and started to diagnose the issue. (b)(3):6(f),(b)(4) also engaged (b)(3):6(f),(b)(4) for assistance in the resolution.
11/11/14	(b)(3):6(f),(b)(4) deployed the Adobe updates via (b)(3):6(f),(b)(4) using a manual packaging process to expedite completion of the updates.
11/11/2014-11/12/2014	(b)(3):6(f),(b)(4) (User Technology Systems Administrator) deployed the Adobe Flash updates to the referenced (b)(3):6(f),(b)(4) servers the night of 11/11.

12. State whether any of the vulnerability scans that LifeLock used detected the older version of Adobe Flash as a potential vulnerability. If so, identify the specific scan(s), provide the date of each such scan, and identify all documents related to each such scan. If LifeLock decided not to address the vulnerability, state the basis for that decision, identify each person involved in that decision, and identify all documents related to that decision.

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

13. Describe in detail how the ransomware attack penetrated and infected LifeLock's computer system(s).

As described above in response to Question 4, the Cryptowall ransomware attack infected LifeLock's system when a LifeLock agent, (b)(3):6(f),(b)(4) logged into REDACTE via a (b)(3):6(f),(b)(4) thin client and was the victim of a malvertising attack. The investigation conducted by (b)(3):6(f),(b)(4) determined that while viewing a website, a malicious flash advertisement was displayed within the browser. The browser was then redirected, without the user's interaction or knowledge, to a malicious website where the Cryptowall payload was downloaded and unpacked into the system memory. Once downloaded, the malware encrypted files onto her Windows session as well as files within her shared network drives (also referred to as the (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4)). For additional detail please see our response to Question 4 above.

14. For each of the infected LifeLock drives, describe the purpose(s) of each drive, identify the network(s) on which each resides, and identify how each drive is mapped.

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

15. Identify any personal information that was held on: (a) LifeLock's (b)(3);6(f),(b)(4), (b) LifeLock's (b)(3);6(f),(b)(4), and (c) each network on which LifeLock's (b)(3);6(f),(b)(4) drive resides.

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

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

- 16. Identify the employee whose local drive was infected. Include in your identification the employee's name, job title, and department.**

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

- 17. Describe what information, including but not limited to member or employee personal information, was accessible to the employee. Include in your description the roles and privileges the employee had in LifeLock's network, as well as the applications and categories of documents and files to which the employee had access rights, and the nature of the access permitted (e.g., read-only or read-write permissions where applicable).**

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

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

18. To the extent LifeLock determined that the ransomware infected only “LifeLock’s (b)(3):6(f),
(b)(4) drives along with one LifeLock Member Services employee’s local drive” describe the basis for that determination. Your description should include, at a minimum, the specific actions LifeLock took in making this determination, an identification of each person involved in that determination, and an identification of all documents relating or referring to that determination.

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

22. Produce all documents identified in response to 1-21 above.

Responsive documents (Bates numbers LIFELOCK-0134241 through LIFELOCK-0134666) are being produced in conjunction with this response.

23. To the extent not produced in response to 22, produce any and all documents referring or relating to the ransomware attack and LifeLock's response thereto, including but not limited to any alerts, incident response reports, third party evaluations, reviews, or assessments, or reports to LifeLock senior management or members of the Board of Directors.

Responsive documents (Bates numbers LIFELOCK-0134241 through LIFELOCK-0134666) are being produced in conjunction with this response.

Please advise whether you have any questions regarding the foregoing; please accord the foregoing information and attached documents confidential treatment under the Commission's Rules of Practice.

Very truly yours,



Andrew G. Berg
Counsel to LifeLock, Inc.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __20__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MEMORANDUM IN SUPPORT OF ITS
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

EXPERT REPORT OF DR. ERIC B. COLE

Table of Contents

Professional Background.....	2
Case Background.....	8
Methodology.....	10
Materials Considered.....	16
Minimum Information Security Standard.....	19
Vulnerability Remediation.....	21
LifeLock Did Not Properly Categorize Its Vulnerabilities, Understating Their Number and Severity.....	24
LifeLock Failed to Remediate, or Timely Remediate, Penetration Test Vulnerabilities	28
LifeLock Did Not Have a Process for Remediating Vulnerabilities in a Timely Manner.....	45
LifeLock Lacked a Process for Applying Patches and Updating Outdated Software in a Timely Manner.....	51
LifeLock Did Not Have Effective Processes for Configuration Management and Password Management.....	69
LifeLock Did Not Have an Effective Process for Documenting Critical Information in Its Database Monitoring and Activity Logs	77
LifeLock’s PCI Assessment and Certification.....	80
PCI AOC Does Not Demonstrate On-Going Compliance.....	80
LifeLock’s July 2013 PCI AOC Was Not Warranted.....	81
LifeLock Did Not Have a PCI Compliant ISP in 2012, 2013, and 2014.....	85
LifeLock’s ISP Deficiencies Enabled the Ransomware Attack in Late 2014.....	87
Conclusion.....	91

Expert Report of Dr. Eric B. Cole
Federal Trade Commission v. LifeLock, Inc., et al.

1. My name is Dr. Eric Cole and I am the principal of Secure-Anchor Consulting, LLC located in Ashburn, Virginia. I am a professional in the field of cyber-security and I was retained by Plaintiff, Federal Trade Commission (FTC), to offer my expert opinion on whether LifeLock, Inc. (“LifeLock”) established, implemented, and thereafter maintained a comprehensive information security program (ISP) designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.¹ My opinion is based on my expertise and over 25 years of experience working with ISPs of organizations in a wide-range of industries (*e.g.*, health care, national retail, financial services and control system environments), including organizations of a similar size (\$300+ million in annual revenue) as LifeLock and with information security needs similar to LifeLock (such as financial institutions needing to protect consumers’ personal information).² My opinion is also based on my experience in leading industry initiatives, creating industry certifications, and developing and teaching curriculum for several core courses for information security professionals at the SANS Institute.
2. I evaluated LifeLock’s information security practices to determine whether LifeLock met the minimum information security standards for organizations of a

¹ I am being compensated \$275.00 per hour by the FTC for my work in this matter.

² While different industries might have different best practices, the core/fundamental security practices are the same across different industries.

similar size and with similar information security needs, not whether LifeLock followed the best practices identified by the information security industry.

3. I also offer my opinion on whether LifeLock's ISP satisfied minimum information security standards for financial institutions.
4. Finally, I offer my opinion on whether LifeLock should have received a Payment Card Information Data Security Standard (PCI DSS) Attestation of Compliance (AOC) in July 2013.

Professional Background

5. I hold a master's degree in computer science from the New York Institute of Technology (1993) and a doctorate in information security from Pace University (2003). I have worked in the cyber and technical information security industry for over 25 years.
6. My education is summarized in my curriculum vitae (CV) attached hereto as Attachment 1 of this Report.
7. I am a contributing author of the report from, and served as a commissioner for, the Commission on Securing Cyberspace for the 44th Presidency.³ I have written multiple books on cyber security including *Network Security Bible - 2nd Edition*, *Advanced Persistent Threat*, and *Insider Threat* which have become cyber security

³ Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency* (2008) <http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf>.

industry standards.⁴ I am one of just 26 members of the Infosecurity Europe Hall of Fame,⁵ an honor requiring professional nomination and election by a panel of industry experts.

8. The details of my publications, including those I have authored within the last 10 years, are summarized in my CV in Attachment 1.
9. I am the founder of Secure Anchor Consulting where I provide cutting edge cyber security consulting services. In addition, I lead research and development initiatives to advance the state-of-the-art in information systems security. In this role and throughout my career, I have performed, and continue to perform, security assessments for organizations, such as financial service organizations that are similar in size to LifeLock and have functions requiring the retention of large amounts of sensitive consumer information.
10. Since 1989, I have been an integral part of The SANS Institute (SANS).⁶ SANS is the largest source for information security training and security certifications in the world. Over 12,000 people a year take courses at SANS, and over 165,000 information security professionals currently participate in SANS programs.⁷

⁴ Eric Cole, *Network Security Bible* (2nd ed. 2009); Eric Cole, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization* (2012); Eric Cole and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft* (2006).

⁵ Infosecurity Europe, *The Infosecurity Europe Hall of Fame* (viewed on Jul. 10, 2015) <<http://www.infosecurityeurope.com/en/education/hall-of-fame-nominations/fame/>>.

⁶ The SANS Institute website (visited Jul. 10, 2015) <<http://www.sans.org/>>.

⁷ The SANS Institute, *About* (visited Jul. 10, 2015) <<http://www.sans.org/about/>>.

11. From 1999 to present, I served as the Dean of Faculty, the Director of Research – Computer Network Attack – Enterprise Security Architecture, and the Director of the Cyber Defense Initiative at SANS. In these roles, I helped design information security curricula, created a degree-granting information security institution, developed several Global Information Assurance Certification (GIAC) certifications, and led industry initiatives such as the top 10/20 vulnerabilities lists and the Cyber defense initiative. I also contributed to the development of several Global Information Assurance Certification (GIAC) certifications including GIAC Certified Security Essentials (GSEC), GIAC Certified Advanced Incident Handling Analysts (GCIH) and GIAC Certified Firewall Analysts (GCFW). GIAC is the industry leading provider of information security certifications.⁸

12. I have authored and taught the *SEC401: Security Essentials* and *SEC501: Advanced Security Essentials – Enterprise Defender* courses at SANS for over 14 years. I have also taught the *SEC566: Implementing and Auditing the Critical Controls – In Depth* course. All of these courses distinguish among minimum, customary, and best practices in information security.

13. I worked as a government employee for 8 years and have worked as a government contractor with several government agencies. I have held various high level security clearances with the United States Department of Defense (DOD), the Central Intelligence Agency (CIA), and the Nuclear Regulatory Commission

⁸ Global Information Assurance Certification website (visited Jul. 10, 2015) <<http://www.giac.org/>>.

(NRC). I have worked for a wide range of government organizations including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), CIA, the United States Department of Energy (DOE), DOD, NRC, and the United States Treasury, including the Secret Service.

14. As a CIA Senior Officer from 1991 to 1996, I was the Program Manager/Technical Director for the Internet Program Team with the Office of Technical Services. The Internet Program Team designed, developed, tested, and deployed internet security products. I designed and developed several secure communication systems and provided technical direction, technical design, security assessments, and programming modules. For the Internet Program Team, I also secured servers to protect them from attack, performed intrusion detection analysis, and reviewed audit logs. While with the Internet Program Team, I performed independent security reviews and penetration testing of World Wide Web servers for other projects and offices within the government. I was responsible for identifying information security weaknesses (such as vulnerability services or unpatched applications) and implementing methods of securing those systems. During my CIA tenure, I received six Exceptional Performance Awards.
15. As a member of the CIA Information Security Assessment Team with the Office of Security, I also evaluated and performed security assessments of network operating systems and identified potential vulnerabilities and ways to remediate those vulnerabilities. For the Office of Security, I also designed a large scale

auditing system with automated review capability and worked on several investigations into viruses that penetrated/attacked CIA systems.

16. From 1999 to 2000, as Chief Information Officer for the American Institutes for Research, I repaired and developed information technology (IT) infrastructures for various organizations such as large academic testing sites. I also provided technical support for the Defense Advanced Research Projects Agency (DARPA), a DOD agency responsible for the development of new technologies for military use.
17. As Chief Scientist and Senior Fellow for Lockheed Martin from 2001 to 2009, I performed research and development to advance the state-of-the-art in Lockheed Martin information systems security. I specialized in: evaluating and designing secure computer networks, network perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I played a lead technical advisory role in multiple high profile security-focused projects for Federal government clients.
18. As Chief Technical Officer for McAfee, from 2009 to 2010, I executed the technology strategy for technology platforms, partnerships, and external relationships for achieving McAfee's goals and business strategies. I worked closely with commercial organizations similar to LifeLock and helped them build out their security programs to protect client information.
19. Since 2010, I have led and been the principal for Secure Anchor Consulting specializing in working with customers to implement effective security solutions.

During this time, I also continued to teach cyber security classes. For both areas, I have been engaged with a variety of customers similar in size and with similar information security needs as LifeLock.

20. I am intimately familiar with the PCI assessment process and the requirements an organization must meet to obtain PCI certification. I have worked with several organizations performing both gap analysis and assisting them in becoming PCI certified. These organizations included financial institutions with net worth greater than \$4 billion in revenue. I have performed over 7 engagements involving PCI over the last several years and all were for entities that were PCI Level 1 like LifeLock.⁹ I have also taught classes and given presentations on PCI.
21. In addition to the PCI work, I have worked with several financial institutions in building minimal baselines of security and referenced architectures for implementing security within these environments. While many financial institutions require additional security measures beyond just the minimal level of security to protect the sensitivity of information, there was always a clear distinction made between the levels of security that were implemented.
22. The details of my work experience and research are summarized in my CV attached as Attachment 1 to this Report.

⁹ Any merchant that process over 2.5 million American Express, 1 million JCB, 6 million Mastercard, or 6 million Visa transactions per year is designated PCI Level 1. *See Auric Systems Int'l., The PCI Standard Simplified* (viewed on Jul. 14, 2015) <<http://www.pcistandard.com/merchant-levels/>>.

23. I have also served as a consultant or expert witness in a number of cases. I have identified the cases in which I have testified either at trial or at a deposition in the past 4 years in my CV attached as Attachment 1 to this Report.

Case Background

24. On March 15, 2010, the United States District Court for the District of Arizona issued a Stipulated Final Judgment and Order (“Order”) in *FTC v. LifeLock, Inc. et al.*, CV-10-000530-PHX-NVW.¹⁰

25. Part II of that Order mandates that LifeLock “establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to the entity’s size and complexity, the nature and scope of the entity’s activities, and the sensitivity of personal information collected . . .”¹¹

26. As part of that ISP, LifeLock must have a program that includes:

* * * *

B. identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the

¹⁰ Att. 2, Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants LifeLock and Davis (ECF No. 9, entered March 15, 2010) (FTC-0002009-29).

¹¹ *Id.* at FTC-0002014.

unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of safeguards put in place to control these risks. . . . ;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, system, and procedures;

* * * *

E. the evaluation and adjustment of [LifeLock's] information security program in light of the results of the testing and monitoring required by Subsection C above of this Section, any material changes to [LifeLock's] operations or business arrangements, or any other circumstances that [LifeLock] know[s] or ha[s] reason to know may have a material impact on the effectiveness of their information security program.¹²

27. I was hired by the FTC to determine whether LifeLock met these requirements.

My opinion and analysis is primarily for LifeLock's ISP from the period of September 2012 through March 2014 because the LifeLock materials that I reviewed and considered were largely restricted to this period. This Report also offers my opinion on whether LifeLock's ISP meets the information security standard that is customary for financial institutions and on whether LifeLock should have received its PCI AOC in July 2013.

¹² *Id.* at FTC-0002014-15.

Methodology

28. I examined LifeLock's ISP using the minimum information security standard. The minimum information security standard is the term I use in this Report to denote the general consensus in the information security industry for the processes that an ISP *must* have to provide the lowest acceptable level of protection to a network from unauthorized access. Without preventing unauthorized access, LifeLock's ISP cannot protect the security, confidentiality, and integrity of its customers' personal information as required by the Order. The required processes cover vulnerability remediation, patching, configuration and password management, and database monitoring. Each of these processes is required to meet the minimum information security standard. These processes are essential for preventing and remediating in a timely manner network vulnerabilities that an attacker could exploit to gain access to the network. The timeframes incorporated into these processes represent the industry consensus on the outside timeframes for correcting vulnerabilities without creating an unreasonable level of risk. No credible argument could be made that an ISP provides an acceptable level of protection without implementing all of the described processes.
29. The minimum information security standard that I use in this Report recognizes that cyber security is not a "one size fits all" approach. For example, a small manufacturer that sells only to retailers would have significantly different levels of acceptable security than a publicly traded company whose business is the protection and control of sensitive consumer information. In choosing the

standard, I first considered that LifeLock's business involves collecting sensitive personal information from consumers. I also considered the size of LifeLock with its \$300 million in annual revenue and over 600 employees. I use in this Report the minimum information security standard for an organization that handles consumers' sensitive personal information and is similar in size to LifeLock. I detail each of these processes encompassed by this standard in the sections below and evaluate whether LifeLock's ISP had these processes in the relevant period.

30. My expertise on the minimum information security standard comes from my education and experience in the information security industry as described in Paragraphs 5 through 23 above and in my attached CV.¹³ Over my 25 years in the industry, I have designed and implemented ISPs and advised numerous clients in managing their ISPs. I have been involved in key industry organizations, am recognized in the industry as one of the leading experts, and maintain regular professional and personal relationships with other leading experts in the industry. All of the foregoing experience gives me a deep understanding of the industry and the industry consensus on the minimally acceptable level of protection for an ISP.

31. All of the processes that I have identified as being part of the minimum information security standard are also covered in the *SEC401: Security Essentials*¹⁴ and *SEC501: Advanced Security Essentials – Enterprise Defender*¹⁵

¹³ Att. 1, Curriculum Vitae of Dr. Eric B. Cole (FTC-0002203-07).

¹⁴ Att. 3, Syllabus for *SEC401: Security Essentials* (FTC-0002208-28).

courses that I developed and have taught at SANS for 14 years. These courses cover the foundational elements of cyber security and distinguish between best practices and the minimum information security standard. A key focus of these courses is understanding the basic level of information security that must be implemented within an organization based on its size and function. The minimum information security standard is also part of the *SEC566: Implementing and Auditing the Critical Controls*¹⁶ course that I teach. The course focuses on assessing an organization and identifying the level of security that should be implemented to properly protect the critical information an organization has at its disposal.

32. These courses reflect the industry consensus on the topics covered. Course curriculum at SANS undergo a robust approval process involving both an initial and annual review by industry experts of the curriculum's technical content to ensure that the curriculum speaks to current industry standards. The different information security professionals who have taught the classes also review the curriculum prior to teaching the classes. For example, over 35 different industry experts have reviewed *SEC401 Security Essentials* as part of the review or teaching process since 2001. I have published papers in academic peer-reviewed journals, and I find the approval process at SANS to be more rigorous.

¹⁵ Att. 4, Syllabus for *SEC501: Advanced Security Essentials – Enterprise Defender* (FTC-0002229-40).

¹⁶ Att. 5, Syllabus for *SEC566: Implementing and Auditing the Critical Security Controls – In-Depth* (FTC-0002241-53).

33. These courses also play a role in propagating the industry consensus as they have been taught to numerous practicing information security professionals. *SEC401 Security Essentials*, for example, has been taught over 500 times to approximately 15,000 students since 2001. The vast majority of the students are people who are either practicing or preparing to practice as information security professionals.

34. I also referenced the following published standards to ensure that the standard used in this Report captures the industry's understanding of the processes necessary for the lowest acceptable level of protection and not best practices:

- *The Critical Security Controls for Effective Cyber Defense 4.0* (“*Critical Security Controls*”);¹⁷
- *PCI Standard version 2.0*; ¹⁸
- *Guide for Assessing the Security Controls in Federal Information Systems and Organizations - NIST Special Publication 800-53A*; ¹⁹

35. The published standards cited above vary in scope and methodology.

Nonetheless, the published standards encapsulate the understanding of certain groups of experts regarding emerging cyber threats and security practices and serve as useful resources to validate the minimum information security standard.

¹⁷ Att. 6, *The Critical Security Controls for Effective Cyber Defense, Version 4.0*, Council on Cyber Security (2012) (FTC-0002254-2342).

¹⁸ Att. 7, *Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, v. 2.0*, PCI Security Standards Council (Oct. 2010) (FTC-0002094-2168).

¹⁹ Att. 8, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, National Institute of Standards and Technology (June 2010) (FTC-0002343-2741).

36. I relied mainly on *Critical Security Controls*. *Critical Security Controls* is an important industry standard for security and protecting computer systems. As stated in its introduction, “[t]he Critical Controls draw on the knowledge gained in combating myriad attacks launched regularly against networks” and represent the efforts of numerous cybersecurity experts and organizations, including the U.S. Department of Defense, the U.S. Computer Emergency Readiness Team, the FBI, and civilian penetration testers.²⁰ These standards are the product of top experts from multiple organizations pooling their extensive first-hand knowledge in defending against actual cyber-attacks to develop a consensus list of defensive techniques to prevent or track them. The *Critical Security Controls* are one of the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced attacks.

37. *Critical Security Controls* provides a comprehensive analysis protocol focusing on core areas: “The Critical Controls represent the sum total of efforts over the last decade to develop standards to identify common vulnerabilities and their severity, define secure configurations, inventory systems and platforms, and pinpoint application weaknesses.”²¹ The prioritized, highly focused components emphasize the base level of security that organizations need to meet. The following are the controls most applicable to my analysis:

²⁰ Att. 6 at FTC-0002256-58.

²¹ *Id.* at FTC-0002257.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs

CSC 16: Account Monitoring and Control

CSC 17: Data Loss Prevention²²

38. For my analysis of LifeLock's 2013 PCI assessment, I relied primarily on PCI Standard Version 2.0 and my extensive experience with the PCI assessment process as detailed in Paragraph 20 above.

39. I also have expertise in the information security practices customarily implemented by financial institutions. My expertise comes from my experience in the information security industry as detailed above, and specifically, from my work in advising financial institution clients in managing their ISPs. Over my career, I have taught and consulted with many of the top financial services organizations on proper methods of implementing effective security. This work has included penetration testing, risk assessments, network architecture design/review, and security assessments. I understand both the challenges and requirements of protecting and securing sensitive client information.

²² *Id.* at FTC-0002254.

Materials Considered

40. My opinions are based on information I have reviewed to date, including the materials referenced herein and in the exhibits attached to this Report, and are based on my knowledge and experience in the fields of computer and network security. I expect to review any reports submitted by LifeLock, and I expressly reserve the right to amend or supplement this Report, as appropriate, after considering the opinions set forth in any such reports or any additional information produced by LifeLock after the date of this Report. For example, if LifeLock has another breach incident similar to the one discovered in November 2014, this information would be used to update and supplement my opinion.

41. I reviewed a large volume of information that LifeLock provided to the FTC for the purpose of describing in detail its ISP, including vulnerability remediation logs, patching logs, and internal emails, reports, and other documents from its information security staff. Although I did not go onsite and perform a full security assessment, these LifeLock documents provided me sufficient evidence of whether its ISP actually performed the processes that constitute the minimum information security standard.

42. I also evaluated security assessments of LifeLock's ISP from three different

organizations:

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

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

I reviewed the methodology summarized in the assessment reports and confirmed that they are consistent with the industry standard for these types of assessments.

43. While the third-party assessments are useful for identifying network vulnerabilities, it is important to note that by their very nature, these assessments cannot provide all of the information necessary to demonstrate compliance with the Order. The assessments provide a snapshot of the vulnerabilities in a network at the time of the assessment. This point-in-time analysis differs from the Order's requirement for an information security *program*, which involves recurring processes defined by policies, supported by technology tools, and actually implemented by staff. To use an illustration, compare a photograph of an office building showing that all of the front doors are closed, and a 24/7 security video of that same building showing the building staff checking and closing any open front doors every hour. The point-in-time assessments are the former; compliance with the Order's ISP provisions requires the latter.
44. A point-in-time analysis, of course, is not irrelevant to evaluating the quality of an ISP. An assessment finding few vulnerabilities in a network could be an indicator that an ISP has all of the processes necessary to meet the minimum security standard. However, some organizations mask their failure to have these processes in place by scrambling to remediate long-outstanding vulnerabilities right before an assessment. These assessment-driven ISPs do not meet the minimum information security standard despite the fact that a particular assessment may show that they did not have many vulnerabilities at the time.
45. I did not see anything in the assessments indicating that the third-party assessors ran any analysis of the vulnerability remediation and patching logs to calculate

how quickly LifeLock responded to discovery of vulnerabilities or release of new patches. Such an analysis is crucial to evaluating LifeLock's performance of the processes required to meet the minimum information security standard.

46. The assessments, however, were useful in identifying vulnerabilities existing at the time of the assessments that suggested a problem with LifeLock's ISP. In general, these vulnerabilities were well-known in the industry and required minimal time and effort to remediate. They would have been remediated if LifeLock's ISP had the basic processes encompassed in the minimum information security standard.
47. Although some of the findings in these assessments sound neutral, and in some instances mildly positive, I would characterize these assessments as some of the more negative that I have seen in my experience of reviewing hundreds of these types of reports. As detailed later in this Report, the negative findings in the assessments are highly specific and focused on deficiencies in significant areas of information security components. In general, these negative findings outweighed the positive or neutral findings in the assessment reports in terms of their value in evaluating the quality of an ISP.
48. In reviewing all of the documents and reports, I found sufficient evidence to understand LifeLock's information security environment and to conclusively determine the ways in which LifeLock fell below the minimum information security standard. A list of the materials I have considered in forming my opinions are cited in this Report and in the attached Appendix.

Minimum Information Security Standard

49. As mentioned, the minimum information security standard is the general consensus in the information security industry for the processes that an ISP *must* have to provide the lowest acceptable level of protection to a network from unauthorized access. The processes must be defined by policy, supported by the necessary technology tools, and actually performed by staff. None of these processes can provide network protection if they either are *ad hoc* or remain just words on a policy document. A brief description of the areas that each process covers is below. A fuller discussion follows with requirements and timeframes specific to organizations similar in size and information security needs as LifeLock.

- *Vulnerability Remediation.* Vulnerabilities are weaknesses in a system that would allow unauthorized system access. A vulnerability is a known exposure in a system that can be used by an adversary as a point of compromise. The longer a vulnerability is not properly fixed or remediated, the greater the exposure of sensitive information. Scanning for vulnerabilities is important, but ultimately, remediating and controlling identified vulnerabilities in a timely manner is what reduces the overall risk of compromise.
- *Patching.* A patch is computer code designed to be inserted into existing software to fix a problem in the software. When a vendor releases a patch, it is announcing that there is a vulnerability in their

software. Therefore, an unpatched system is in a *known* exposed state because patches are publicly available to both organizations and potential attackers. The longer a system is not patched, the greater the exposure and risk of compromise. The same analysis applies when vendors release new versions of a software. Vendors often stop supporting older versions of software and release new versions to address known vulnerabilities. To maintain a secure network, an organization must apply patches and install new versions in a timely manner.

- *Configuration and Password Management.* Changes in the network, such as the installation of new software or patches, could create vulnerabilities if not properly managed. For example, installing new software could introduce unneeded services or vendor default parameters that attackers could exploit to gain unauthorized access to the network. For these reasons, an organization must properly track any changes to the network, test the changes, and take the remediation steps necessary (such as removing the unneeded service or changing the default parameters in the preceding example) to ensure that the changes do not degrade the level of network security. In addition, an organization must manage password access to network resources so that employees' use of weak passwords does not compromise an otherwise well-configured network.

- *Database Monitoring and Documentation.* Even a secure network will face intrusions, so an organization must have the ability to monitor for such intrusions. If an organization does not monitor, it will not be able to stop or mitigate an attack in a timely manner. An organization must also have the ability to monitor its vulnerability remediation, patching, and configuration and password management processes to ensure that they are running properly. Critical to effective monitoring is consistent documentation of the activities involved in each of these processes. Without consistent documentation, an organization will not have information of sufficient quality or detail to evaluate the performance of its ISP and make necessary adjustments.

Vulnerability Remediation

50. The minimum information security standard requires implementation of a formal vulnerability remediation process. Vulnerabilities are weaknesses in a system that an attacker could exploit to obtain unauthorized access to the system. The vulnerability remediation process must have a comprehensive scanning protocol for regularly scanning the system for vulnerabilities. *Critical Security Controls* requires running scans “on a weekly or more frequent basis.”²³ PCI DSS requires scans less frequently, on a quarterly basis and whenever any significant changes

²³ Att. 6, *The Critical Security Controls for Effective Cyber Defense, Version 4.0, Council on Cyber Security (2012)* at FTC-0002275.

occur in the network.²⁴ In my expert opinion and experience, PCI DSS represents the minimum level of scanning for systems that contain or have access to sensitive information.

51. Generating a large number of vulnerabilities through scans, however, is ineffective without a robust process for categorizing each vulnerability, prioritizing each vulnerability based on the criticality of the security risk posed, allocating resources so that the vulnerability can be fixed, and verifying the vulnerability has been resolved. Vendors often provide a criticality rating of the vulnerabilities present in their software using their own rating system; the National Vulnerability Database (NVD) uses a separate rating system called the Common Vulnerability Scoring System (CVSS) to provide a criticality rating.²⁵ An organization must take the baseline vulnerability ratings provided by the vendors and NVD and determine whether to adjust the rating to account for the peculiarities of their network. For instance, a vulnerability with a medium level of criticality may require an upgrade to a high level of criticality if the vulnerability is on an extremely sensitive system.

²⁴ Att. 7, *Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, v. 2.0*, PCI Security Standards Council (Oct. 2010) (FTC-0002094-2168) at FTC-0002153.

²⁵ The NVD is part of the National Institute for Standards and Technology (NIST) and is the U.S. government repository of standards based vulnerability management data. Two common uses of CVSS are prioritization of vulnerability remediation activities and calculation of the severity of vulnerabilities discovered on one's systems. The NVD provides CVSS scores for almost all known vulnerabilities. For each vulnerability, NVD assigns numeric CVSS scores and corresponding severity rankings of "Low" (0.0 to 3.9), "Medium" (4.0 to 6.9), and "High" (7.0 to 10.0). See National Institute of Standards and Technology, *NVD Common Vulnerability Scoring System Support v2* (visited Jul. 10, 2015) <<https://nvd.nist.gov/cvss.cfm>>.

52. The process must ensure that all of these steps, from discovery of the vulnerability to verification of remediation, are completed within a timeframe that does not place the network at an unreasonable risk of attack. LifeLock's policy as of July 1, 2013, states that vulnerabilities it rates as Critical should be remediated within 30 days, High within 60 days, and Medium/Low within 90 days.²⁶ These timeframes match the minimum information security standard. After the vulnerability has been fixed, retesting and follow-up are necessary to ensure that vulnerabilities stay remediated.

53. A vulnerability remediation program must also fully document each step of the remediation process. For each vulnerability, the documentation must provide a description, the date of discovery, the date a vulnerability remediation ticket was created, the date and description of all remediation efforts, and the date the remediation was validated. If an organization decides either to downgrade the criticality of a vulnerability or to not remediate a vulnerability at all, it must justify that decision by documenting the rationale. The documentation must clearly show the risk analysis performed and the remediation measures in place to reduce the risk to an acceptable level.

54. The documentation process is crucial to the vulnerability remediation program. Without proper documentation, an organization is essentially blind, having no reliable way of tracking the progress of efforts to remediate vulnerabilities. An

²⁶ Att. 9, Email from (b)(3):6(f),(b)(4) et al. (July 1, 2013) (LL-0053865-66).

organization cannot effectively make the decisions necessary to remediate vulnerabilities without consistent, detailed documentation of its remediation efforts.

55. As explained in more detail below, LifeLock did not have a vulnerability remediation process meeting the minimum information security standard. LifeLock's documents, including its vulnerability remediation logs and internal emails, demonstrate a consistent pattern of numerous vulnerabilities throughout its network, inconsistent or ad hoc tracking of vulnerability remediation requests (VRR),²⁷ significant delays remediating vulnerabilities (including those identified by penetration tests and required by its 2013 PCI assessor for remediation), and incomplete documentation of its remediation efforts.

56. LifeLock's failures were consistent and widespread, and in my professional opinion, render their ISP well below the minimum information security standard.

LifeLock Did Not Properly Categorize its Vulnerabilities, Understating Their Number and Severity

57. Internal emails from LifeLock's onsite information security consultant reveal that by January 2013, LifeLock had thousands of high priority vulnerabilities that it

²⁷ Vulnerability remediation requests, or VRRs, are service tickets that LifeLock creates for network vulnerabilities to initiate and track remediation efforts.

masked by: (a) grouping multiple vulnerabilities as a single VRR; and/or (b) unilaterally downgrading the vulnerabilities to low priority.²⁸

58. On January 17, 2013, LifeLock's information security consultant, Gwen Ceylon, emailed LifeLock's Senior Director of Infrastructure, Director of Infrastructure, and Internal Auditor to explain that although there appeared to be approximately 200 VRRs in the LifeLock's vulnerability remediation management system, that was not the reality as there were currently "4669 vulnerabilities on the systems in the PCI environment. Most of them are ranked critical."²⁹ Specifically, Ms. Ceylon identified 2,906 vulnerabilities ranked "high" in LifeLock's PCI environment, when applying the Common Vulnerability Scoring System (CVSS) score of 7-10.³⁰ Vulnerabilities with a CVSS "high" ranking are considered in the information security industry to be critical vulnerabilities requiring priority remediation.

59. In addition to lumping vulnerabilities together, LifeLock would downgrade the criticality of vulnerabilities without documented justification. Ms. Ceylon explained that Information Security staff VRRs would often contain multiple vulnerabilities and that LifeLock Information Security staff had set the VRR ticket

²⁸ Att. 10, Email from Gwen Ceylon to Tony Valentine (Jan. 17, 2013) (LIFELOCK-0085248-50); Att. 11, Email from Gwen Ceylon to Tony Valentine (Jan. 7, 2013) (LIFELOCK-038588-89).

²⁹ Att. 10 at LIFELOCK-0085248.

³⁰ *Id.* at LIFELOCK-0085250 ("Overview Charts" worksheet).

priority to low.³¹ Likewise, in an earlier email, Ms. Ceylon told the Internal

Auditor that:

A bunch of Microsoft vulnerabilities -- VRR went in as low. But note that the actual risk ranking from the scan engine (which comes from the industry standard Mitre/NIST CVE scores and based on what Microsoft says) is critical and severe. This VRR is a week from being late. They can't just lower the risk ranking to avoid patching systems.³²

Included in this VRR were 20 Microsoft patches, 14 of which were ranked by Microsoft as "critical" and 6 of which were ranked "important."³³ Nonetheless, the VRR priority assigned by Information Security staff was "low."³⁴ Although detected on an October 11, 2012 scan, a VRR was not created until October 29, 2012 and was not closed until May 15, 2013, based on a March 26, 2013 scan.³⁵

³¹ *Id.* at LIFELOCK-0085248.

³² Att. 11 at LIFELOCK-0038588.

³³ *Id.* at LIFELOCK-0038588-89; Att. 12, Email from (b)(3);6(f),(b)(4) to Austin Appel (Jun. 06, 2013) (LIFELOCK-0030131-32). The "critical" Microsoft patches were MS10-077, MS11-028, MS11-039, MS11-078, MS11-100, MS12-016, MS12-025, MS12-035, MS12-036, MS12-038, MS12-045, MS11-044, MS12-052, and MS12-054. The "important" Microsoft patches were MS12-048, MS12-041, MS12-047, MS12-049, MS12-055, and MS12-056. See Microsoft Corporation, *Security Advisories and Bulletins* (viewed on Jul. 11, 2015) <<https://technet.microsoft.com/library/security/>>.

³⁴ Att. 12; Att. 13, LifeLock's VRR Logs (322 Open Requests WO Tables with Notes, generated by (b)(3);6(f),(b)(4) (May 27, 2015); VRRs – June 2012 to September 2012 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – October 2012 to March 2013 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – April 2013 to December 2014 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – April 2012 to May 2015 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – April 2012 to May 2015 WO Table with Notes and Priority, generated by (b)(3);6(f),(b)(4) (May 29, 2015)) (LIFELOCK-0135783-86, 0138077-78) at LIFELOCK-0135785 (line 143).

³⁵ Att. 13 at LIFELOCK-0135785 (line 143).

Even accepting the March 26, 2013 date, that is over five months after detection, well beyond the timeframe for remediating critical and high vulnerabilities.

60. LifeLock's 2013 PCI Assessor, (b)(3);6(f),(b)(4) apparently discovered this downgrading practice in conducting its PCI review, noting that an Information Security employee had "unilaterally downgraded [a] Critical patch."³⁶ As a result, the PCI Assessor required that LifeLock provide evidence that there was now a documented process in place for downgrading a "Critical" vulnerability, and that if downgrades had occurred since the implementation of the documented process, LifeLock provide "evidence of the non-unilateral decision."³⁷

61. On July 1, 2013, in an email to all remediation teams, LifeLock announced it was changing the VRR process to eliminate the ability to unilaterally downgrade criticality ratings generated by the automated scans, instead "using the criticality rating as dictated by the (b)(3);6(f),(b)(4) service" and only allowing a downgrade upon a formal request with a business justification.³⁸

62. LifeLock's detailed logs of closed VRR activities confirm these internal emails.³⁹ The logs contain unrealistically few vulnerabilities identified as Critical or High for significant periods of time, specifically from September 1, 2012 to February

³⁶ Att. 14, LifeLock, Inc., PCI Audit Augmented Punch List (June 11, 2013) (LIFELOCK-0039701-07) at LIFELOCK-0039705.

³⁷ *Id.*

³⁸ Att. 9 at LIFELOCK-0053865.

³⁹ Att. 13.

21, 2013, and from March 13, 2013 to June 25, 2013.⁴⁰ During those two periods, the logs do not contain any Critical and just two High vulnerabilities. These months-long gaps with no Critical or High vulnerabilities are highly unlikely and strongly suggest that LifeLock was downgrading the criticality rating as indicated in the emails.

63. Arbitrarily lumping multiple vulnerabilities into a single VRR and downgrading criticality ratings without any formal process artificially decrease the number of serious vulnerabilities existing in a network. Such practices serve only to prevent the effective operation of the vulnerability remediation process and therefore render LifeLock's ISP below the minimum security standard.

LifeLock Failed to Remediate, or Timely Remediate, Penetration Test Vulnerabilities

64. In November 2012, (b)(3) 6(f),
(b)(4) rated LifeLock's internal network as "Below Average" and identified "Patch and Vulnerability Management" as a major problem area for LifeLock. (b)(3) 6(f),
(b)(4) explained that it "observed vulnerability trends across multiple information system. . . . [that] can be attributed to a weak patch and vulnerability management process, or to a weak implementation of (or gaps in) said process."⁴¹

⁴⁰ Att. 27, Declaration of Elizabeth Anne Miles Pursuant to 28 U.S.C. § 1746 (FTC-0002742-2851) at FTC-0002747.

⁴¹ Att. 15, *LifeLock, Inc.: Information Assurance Services Enterprise Security Assessment*, (b)(3) 6(f), (b)(4) (Nov 13, 2012) (LIFELOCK-0053403-61) at LIFELOCK-0053407, 0053449.

65. A striking example of LifeLock’s vulnerability remediation management failures is found in its response to vulnerabilities identified in late 2012 penetration tests. By July 2013, LifeLock had not yet remediated all of the vulnerabilities identified by the penetration tests and only attempted to do so when their PCI assessor, (b)(3);6(f),(b) demanded proof of their remediation during the PCI certification process.⁴² Although the PCI assessor ultimately adopted LifeLock’s claim that it “corrected and retested” the vulnerabilities identified by (b)(3);6(f),(b)(4)⁴³ the evidence provided by LifeLock demonstrates otherwise.⁴⁴

66. The following page from LifeLock’s 2013 PCI Report on Compliance (“PCI RoC”) has the list of vulnerabilities that LifeLock claimed to have remediated (corrected and retested):⁴⁵

⁴² Att. 16, Email from (b)(3);6(f),(b)(4) *et al.* (Jul. 16, 2013) (LIFELOCK-0025172-74).

⁴³ Att. 17, PCI Report on Compliance for LifeLock, (b)(3);6(f),(b)(4) (July 2013) (LIFELOCK-0097021-229) at LIFELOCK-0097204-05.

⁴⁴ LifeLock’s failure to correct and retest the penetration test vulnerabilities is one of the reasons it should not have received its PCI AOC in 2013. *See infra* ¶¶ 152-157.

⁴⁵ Att. 17 at LIFELOCK-0097204-05.

PCI REPORT ON COMPLIANCE FOR LIFELOCK

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	(b)(3):6(f),(b)(4)	Yes		(b)(3):6(f),(b)(4)
		Yes		

Confidential and Proprietary Information: Need to Know

183

July 2013

PCI REPORT ON COMPLIANCE FOR LIFELOCK

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

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Comments
	(b)(3):6(f),(b)(4)			(b)(3):6(f),(b)(4)
		Yes		
11.3.1 Network-layer penetration tests		Yes		
11.3.2 Application-layer penetration tests		Yes		

Confidential and Proprietary Information: Need to Know

184

July 2013

67. I examined the documents LifeLock provided to (b)
(3):6
(f)(b)(v) as “documenting” that LifeLock “corrected and retested” these penetration test vulnerabilities.⁴⁶ The documents do not substantiate that these were remediated, and other internal documents establish that a number of them were not “corrected and retested” until well after July 2013.

68. Internal emails in October 2013⁴⁷ and November 2013⁴⁸ show that some of these vulnerabilities had not been addressed almost a year after being identified. The October 2013 email states, “These are vulnerabilities that were identified in assessments completed in September and November 2012 **and should have been remediated months ago.**” (Emphasis supplied.)⁴⁹

69. LifeLock even admitted in its responses to the FTC’s information requests that a number were “closed... without documentation of evaluation.”⁵⁰ In September 2014, almost two years after the penetration tests identified the vulnerabilities, 4 vulnerabilities remained unremediated. Three of these VRRs - 81915 (Cookie

⁴⁶ Att. 18, LifeLock’s Documentation of Penetration Test Vulnerability Remediation Submitted to (b)(3):6(f),(b)(4) (submitted Jul. 2013) (LIFELOCK-00132479-516).

⁴⁷ Att. 19, Email from AnneMarie Olson to Michele Grant and (b)(3):6(f),(b)(4) (Oct. 11, 2013) (LIFELOCK-0081949-56).

⁴⁸ Att. 20, Email from Austin Appel to (b)(3):6(f),(b)(4) (Nov. 5, 2013) (LIFELOCK-0032898-99) (categorizing vulnerabilities identified in 2012 penetration tests as “[t]ickets we don’t know status on”, “[t]ickets that are waiting on us”, or “tickets waiting on other teams”).

⁴⁹ Att. 19 at LIFELOCK-008194.

⁵⁰ Att. 21, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Attorney, Federal Trade Commission (Sept. 19, 2014) (LIFELOCK-0110772-81) at LIFELOCK-0110774-75. The specific VRRs that were closed without documentation of evaluation are VRR Nos. 81911, 81915, 81916, and 81932.

Settings), 81916 (HTTP Response), and 81932 (Clickjacking) - were reopened by LifeLock after being previously “closed... without documentation of evaluation.”⁵¹ As (b)(3):6(f), (b)(4) explained in September 2012, these three vulnerabilities would have required “minimal” effort for LifeLock to remediate.⁵²

70. LifeLock closed the fourth, VRR 81911 (Disable Auto Complete), after erroneously concluding that it could not disable the Auto Complete function. The Auto Complete function automatically populates fields on a webpage using information that a user had previously inputted. An attacker accessing a user’s browser would then be able to use the Auto Complete function to login to restricted sites as the user. LifeLock closed this VRR after concluding that this function could only be turned off by the individual user.⁵³ This is plainly wrong. LifeLock could have turned off this function using the application setting with minimal effort. Both this vulnerability and its remediation are well-known in the industry.

71. For the other vulnerabilities, the documents LifeLock provided (b)(3):6 (b)(4) do not show that LifeLock “corrected and retested” the vulnerabilities. In most instances, the documents are notations that an action was taken without attaching any corroborating documentation, such as documented steps that were taken,

⁵¹ *Id.*

⁵² Att. 22, *LifeLock: Information Assurance Services. Enterprise Security Assessment Report - Portal*, (b)(3):6(f),(b)(4) (Sept. 12, 2012) (LIFELOCK-2081-122) at LIFELOCK-2104-110, 2114.

⁵³ Att. 21 at LIFELOCK-0110774.

screenshots to prove that the changes were made, and documented tests to show the vulnerabilities were actually fixed.⁵⁴

72. Even crediting LifeLock's uncorroborated assertions that it corrected and retested the penetration test vulnerabilities, the documents it provided to (b) (3), (6), (f) show that "remediation" took over 4 months after they were identified in the penetration tests for all but two of the vulnerabilities. As LifeLock acknowledged in July 2013, and as required by the minimum information security standard, Critical vulnerabilities should be remediated in 30 days, High in 60 days, and Medium/Low in 90 days.⁵⁵ The table in the following pages summarizes LifeLock's remediation efforts as described in its "corrected and retested" documents with respect to each of the penetration test vulnerabilities:

⁵⁴ Att. 18.

⁵⁵ Att. 9, Email from (b)(3);6(f),(b)(4) et al. (July 1, 2013) (LIFELOCK-0053865-66).

VRR Ticket Number	Documentation Supports Corrected and Retested?	Penetration Test	Description of Vulnerability	LL Priority Designation	Date Corrected and Retested Documentation Shows Purportedly Resolved	Time to LifeLock Claimed Resolution from Penetration Test Discovery
81253	No. Documentation does not show vulnerability was corrected and retested.	(b)(3):6(f),(b)(4)	SNMP community strings can be used to gain access to a system	Low	March 26, 2013.	Over 4 months. ⁵⁶
81254	No. Documentation does not show vulnerability was corrected and retested.		SNMP community strings can be used to gain access to a system	Low	March 26, 2013.	Over 4 months.
81256	No. Documentation does not show vulnerability was corrected and retested.		SNMP community strings can be used to gain access to a system	Low	March 25, 2013.	Over 4 months.
81262	No. Documentation does not show vulnerability was corrected		SNMP community strings can be used to gain access to a	Low	March 26, 2013.	Over 4 months.

⁵⁶ VRRs 81253, 81254, 81256, and 81262 were initially discovered by an October 11, 2012 Internal PCI scan, so they were actually unresolved for a longer period than indicated in the table above. See Att. 13, LifeLock's VRR Logs (322 Open Requests WO Tables with Notes, generated by (b)(3):6(f),(b)(4) (May 27, 2015); VRRs – June 2012 to September 2012 ARC Table with Notes, generated by (b)(3):6(f),(b)(4) (May 29, 2015); VRRs – October 2012 to March 2013 ARC Table with Notes, generated by (b)(3):6(f),(b)(4) (May 29, 2015); VRRs – April 2013 to December 2014 ARC Table with Notes, generated by (b)(3):6(f),(b)(4) (May 29, 2015); VRRs – April 2012 to May 2015 ARC Table with Notes, generated by (b)(3):6(f),(b)(4) (May 29, 2015); VRRs – April 2012 to May 2015 WO Table with Notes and Priority, generated by (b)(3):6(f),(b)(4) (May 29, 2015)) (LIFELOCK-0135783-86, 0138077-78) at LIFELOCK-081253 (lines 1042, 1044, 1048, 1052).

	and retested.		system			
81592	No. Documentation does not show vulnerability was corrected and retested.	(b)(3) 6(f), (b)(4)	Open SSL and Apache update missing	Low	Never.	Documentation indicates unresolved.
81911	No. Documentation does not show vulnerability was corrected and retested.		Disable auto complete	High	Never.	Never.
81913	No. Documentation does not show vulnerability was corrected and retested.		Caching directory issue	High	November 28, 2012.	2 weeks.
81915	No. Documentation does not show vulnerability was corrected and retested.		Cookie setting	High	Never.	Never.
81916	No. Documentation does not show vulnerability was corrected and retested.		HTTP response information disclosure	High	Never.	Never.
81926	No. Documentation does not show vulnerability was corrected and retested.		Hidden directory enumeration	High	Never.	Never.
81932	No. Documentation does not show vulnerability was corrected and retested.		No clickjacking protection	High	Never.	Never.

83219	No. Documentation does not show vulnerability was corrected and retested.	(b)(3),6(f),(b)(4)	Directory traversal	High	Never.	Documentation indicates unresolved.
83228	No. Documentation does not show vulnerability was corrected and retested.		Local admin password	Medium	April 4, 2013.	Almost 5 months.
83232	No. Documentation does not show vulnerability was corrected and retested.		Guessable Tomcat manager credentials	High	April 2, 2013.	Almost 5 months.
83627	No. Documentation does not show vulnerability was corrected and retested.		Web VPN – no longer needed?	Low	March 15, 2013.	Over 4 months.
83629	No. Documentation does not show vulnerability was corrected and retested.		Check_MK – no authentication	Low	March 19, 2013.	Over 4 months.
83631	No. Documentation does not show vulnerability was corrected and retested.		(b)(3),6(f),(b)(4) information disclosure	Low	December 20, 2012.	5 weeks.

73. Directory Traversal (VRR 83219), Local Administrator Password Reuse (VRR 83228), and Default or Guessable Tomcat Manager Credentials (VRR 83232) were all identified by [REDACTED] as “High” severity vulnerabilities with CVSS scores of 10.⁵⁷ LifeLock’s response to these three vulnerabilities demonstrates the deficiencies in its vulnerability remediation management.

74. *Directory Traversal – VRR 83219.* Normally, an organization would implement strict access controls in order to limit a user accessing an application on its website to files located in the web server’s document root. A Directory Traversal vulnerability allows the user to potentially read files outside the web server’s document root. The document root provides access to the entire storage device that contains all of the sensitive information. Based on the server it was identified on, this could lead to exposure of sensitive information. A storage device contains information in a hierarchy fashion, with the root being the top of the tree. Someone who can access the root has access to all of the information that resides below it. In its November 2012 penetration test, [REDACTED] exploited this vulnerability to gain control of the [REDACTED] domain.⁵⁸ A domain is a group of systems that can access each other’s resources. If an adversary can gain control of a domain, they would be able to potentially access all of the data that resides on those systems and exploit sensitive information.

⁵⁷ Att. 15, *LifeLock, Inc.: Information Assurance Services Enterprise Security Assessment*, [REDACTED] (Nov 13, 2012) (LIFELOCK-0053403-61) at LIFELOCK-0053421-23.

⁵⁸ Att. 15 at LIFELOCK-0053408, 0053421, 0053430-437.

75. (b)(3);6(f),
(b)(4) identified *Directory Traversal* as a High severity vulnerability with an estimated **CVSS score of 10**.⁵⁹ LifeLock's response to this vulnerability was as follows:

- Although identified in the November 13, 2012 (b)(3);6(f),
(b)(4) Report as a High severity vulnerability with an estimated CVSS score of 10, a VRR was not submitted until December 6, 2012, over 3 weeks later;⁶⁰
- Notwithstanding its "high" priority VRR designation by the Director of Information Security on December 6, 2012, with an assigned due date of December 26, 2012, LifeLock's first identified action takes place March 20, 2013, approximately three and a half months later;⁶¹
- On March 20, 2013, LifeLock noted the problem was related to an outdated application that could not be updated and asked if the server was still required;⁶²
- Over two months later, on May 31, 2013, LifeLock indicated the server was still needed;⁶³
- One month later, July 1, 2013, LifeLock staff suggested a possible solution but explained that he was uncertain how to proceed;⁶⁴

⁵⁹ *Id.* at LIFELOCK-0053421.

⁶⁰ Att. 13 at LIFELOCK-0138078 (line 117).

⁶¹ Att. 23, Email from Jenner Holden to (b)(3);6(f),(b)(4) (Dec. 6, 2012) (LIFELOCK-0089119-120).

⁶² Att. 13 at LIFELOCK-0138078 (lines 117, 118).

⁶³ *Id.* at LIFELOCK-0138078 (line 119).

⁶⁴ *Id.* at LIFELOCK-0138078 (line 120).

- On July 19, 2013, the PCI RoC identified the issue as corrected and retested, but the reportedly supporting documentation only notes the uncertain status of this VRR as of July 1, 2013 without any indication it has been corrected and retested;⁶⁵
- Finally, on July 31, 2013, LifeLock staff note “both url’s return 404 errors” indicating the issue has been resolved.⁶⁶

For this high priority penetration test vulnerability, LifeLock took over 3 weeks to submit a remediation request, over 3 months from that point to begin working on the vulnerability and discovering there was an outdated application, more than an additional two months to confirm the server involved was still needed, another month to propose a potential solution, and yet another month to provide any confirmation that a solution had been implemented.

76. Because of delays in ticketing after detection, initially responding to this high priority VRR, evaluating the need for the server, identifying a solution, and implementing and verifying the solution, it was **over 8 months** between identification and “verification” of resolution.⁶⁷

77. If this were a brand new vulnerability without a known solution, it would be conceivably reasonable that the fix was not timely implemented. But that is not

⁶⁵ Att. 18 at LIFELOCK-0132503-04.

⁶⁶ Att. 13 at LIFELOCK-0138078 (line 121).

⁶⁷ As discussed below, LifeLock’s configuration management issues are significant. If LifeLock had followed basic security principles, such as system hardening or configuration management, this problem could have easily been avoided all together.

the case. Directory Traversal vulnerabilities have been a known problem since the late 1990s, and every web server software supports the ability to remediate this vulnerability.

78. *Local Administrator Password Reuse – VRR 83228*. User credentials, which include a user name and a password, allow system access. If a password is easy to guess, or the same password is used for every system, it provides an attacker the opportunity to gain system access. Passwords must be periodically changed to minimize or reduce the chance of compromise. Administrative or manager credentials are extremely sensitive in computer systems because, if compromised, they allow an adversary significant control over the system.

79. Manager credentials can be used to gain access to a system. A local administrator is similar to a store manager, with privileged access and the ability to see what people are doing throughout the store. In a computer system, a manager has the same level of visibility to access some information on the system, including reading, changing or deleting information.

80. (b)(3);6(f),
(b)(4) identified *Local Administrator Password Reuse* as a High severity vulnerability, with a **CVSS score of 10**, and identified the issue as “Enterprise-wide.”⁶⁸ In its November 2012 penetration test, (b)(3);6(f),
(b)(4) exploited this

⁶⁸ Att. 15 at LIFELOCK-0053422.

vulnerability to gain control of the (b)(3):6(f),(b)(4) domain.⁶⁹ LifeLock's response to this vulnerability was as follows:

- Although identified in the November 13, 2012 (b)(3):6(f),(b)(4) Report as a High severity vulnerability with a CVSS score of 10, a VRR was not submitted until December 6, 2012, over three weeks later;⁷⁰
- Notwithstanding its “medium” priority VRR designation by the Director of Information Security on December 6, 2012, with an assigned due date of January 15, 2012, LifeLock's first identified action takes place March 20, 2013, three and a half months later;⁷¹
- On March 20, 2013, over four months after the (b)(3):6(f),(b)(4) report, LifeLock staff noted that it had implemented (b)(3):6(f),(b)(4) recommendation and “[u]pdated both default domain GPO's for the local administrator to authenticate over the network”;⁷²
- On April 4, 2013, a LifeLock Information Security staffer notes, “Verified manually that the ‘Deny access from the network’ GPO setting was successfully propagated. Will investigate using unique local administrator passwords in the future”;⁷³

⁶⁹ *Id.* at LIFELOCK-0053408, 0053422, 0053430-437.

⁷⁰ Att. 13 at LIFELOCK-0138077 (line 1257).

⁷¹ Att. 24, Email from (b)(3):6(f),(b)(4) to Jenner Holden (Dec. 6, 2012) (LIFELOCK-0088573-74).

⁷² Att. 13 at LIFELOCK-0138077 (line 1257).

⁷³ *Id.*

- On July 19, 2013, the PCI RoC identified the issue as corrected and retested, but the reportedly supporting documentation only included LifeLock staff's notes without any documentation that it has been retested beyond a manual verification;⁷⁴
- LifeLock's documents do not identify what, if anything, resulted from Information Security staff's plan to explore using "unique local passwords in the future."⁷⁵

For this High severity penetration test vulnerability, LifeLock took over 3 weeks to submit a remediation request, over 3 months from that point to begin working on the issue, and almost 4 months to purportedly resolve the issue.

81. Because of delays in ticketing after detection, initially responding to a medium priority VRR, and implementing and verifying the solution, it was 4.5 months between identification and purported resolution, even accepting that LifeLock's manual verification was sufficient to resolve this Enterprise-wide issue.

82. *Default or Guessable Tomcat Passwords – VRR 83232.* Having guessable manager credentials means an attacker could easily figure out the password, login as a manager and gain manager access to the system. Tomcat is a web server that

⁷⁴ Att. 18, LifeLock's Documentation of Penetration Test Vulnerability Remediation Submitted to (b)(3);(b)(6);(b)(4) (submitted Jul. 2013) (LIFELOCK-00132479-516) at LIFELOCK-0132505. While a manual verification can be acceptable, documentation and proof of the change is necessary.

⁷⁵ Att. 13 at LIFELOCK-0138077 (line 1257). This suggests LifeLock was still using local administrator password at that time and had not systematically resolved the issue by ceasing use of local administrator passwords Enterprise-wide.

provides front-end access to back-end databases containing sensitive information. Guessable manager credentials make it easier for an attacker to login to Tomcat as a manager and access sensitive information on the back-end databases. In this instance, (b)(3);6(f), (b)(4) found one of the login credentials was (b)(3);6(f),(b)(4). This is a well-known vulnerability in the information security industry with a simple and easy solution – using non-guessable, unique passwords.

83. (b)(3);6(f), (b)(4) identified *Default or Guessable Tomcat Passwords* as a High severity vulnerability with an estimated **CVSS score of 10**.⁷⁶ In its November 2012 penetration test, (b)(3);6(f), (b)(4) exploited this vulnerability to launch a successful attack.⁷⁷ LifeLock’s response to this vulnerability was as follows:

- Although identified in the November 13, 2012 (b)(3);6(f), (b)(4) Report as a High severity vulnerability with an estimated CVSS score of 10, a VRR was not submitted until December 6, 2012, over 3 weeks later;⁷⁸
- Notwithstanding its “high” priority VRR designation by the Director of Information Security on December 6, 2012, with an assigned due date of

⁷⁶ Att. 15 at LIFELOCK-0053423.

⁷⁷ *Id.* at LIFELOCK-0053409, 0053423, 0053437-440.

⁷⁸ Att. 13, LifeLock’s VRR Logs (*322 Open Requests WO Tables with Notes*, generated by (b)(3);6(f),(b)(4) (May 27, 2015); *VRRs – June 2012 to September 2012 ARC Table with Notes*, generated by (b)(3);6(f),(b)(4) (May 29, 2015); *VRRs – October 2012 to March 2013 ARC Table with Notes*, generated by (b)(3);6(f),(b)(4) (May 29, 2015); *VRRs – April 2013 to December 2014 ARC Table with Notes*, generated by (b)(3);6(f),(b)(4) (May 29, 2015); *VRRs – April 2012 to May 2015 ARC Table with Notes*, generated by (b)(3);6(f),(b)(4) (May 29, 2015); *VRRs – April 2012 to May 2015 WO Table with Notes and Priority*, generated by (b)(3);6(f),(b)(4) (May 29, 2015)) (LIFELOCK-0135783-86, 0138077-78) at LIFELOCK-0138078 (line 123).

December 26, 2012, LifeLock's first identified action takes place March 27, 2013, over three and a half months later;⁷⁹

- On March 27, 2013, LifeLock noted it had removed the default credentials, “[u]pdated the (b)(3);6(f),(b)(4) file,” and was waiting for Tomcat to reboot so that these fixes could be applied;⁸⁰
- On April 2, 2013, LifeLock staff simply state “[t]his has been resolved” without any further explanation;⁸¹
- On July 19, 2013, the PCI RoC identified the issue as corrected and retested, but the reported supporting documentation only included LifeLock staff's notes without any documentation it had been retested;⁸²
- Not until May 6, 2015⁸³ does LifeLock verify its resolution, citing to an October 22, 2013 internal PCI scan as verifying the issue was resolved.⁸⁴

For this high priority penetration test vulnerability, LifeLock took over 3 weeks to submit a remediation request, over 3 months from that point to begin working on the issue, almost 4 months to purportedly resolve the issue, and over **two more years** to confirm its resolution.

⁷⁹ Att. 25, Email from (b)(3);6(f),(b)(4) to Jenner Holden (Dec. 6, 2012) (LIFELOCK-0089186-87).

⁸⁰ Att. 13 at LIFELOCK-0138078 (line 123).

⁸¹ *Id.* at LIFELOCK-0138078 (line 124).

⁸² Att. 18 at LIFELOCK-0132506-08.

⁸³ Due to the FTC's investigation, LifeLock apparently began trying to find documentation of its activities for many outstanding vulnerabilities in May 2015.

⁸⁴ Att. 13 at LIFELOCK-0138078 (line 124).

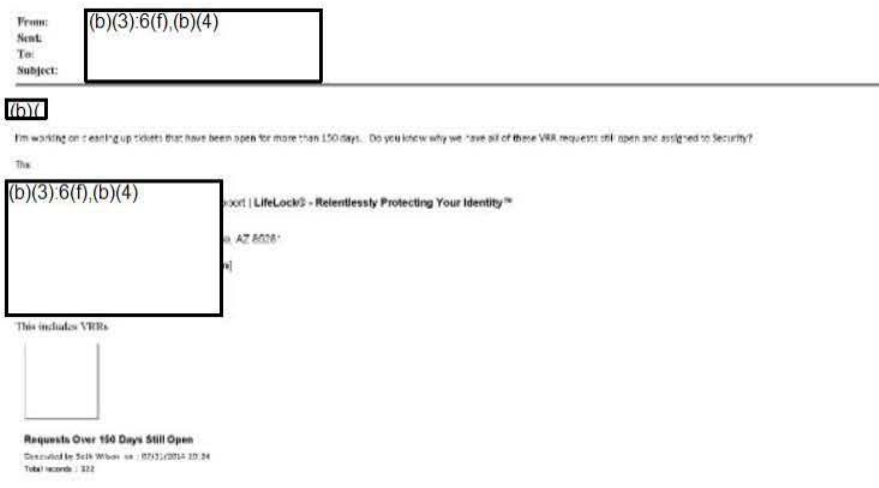
84. LifeLock knew these vulnerabilities were given (b)(3) 6(f), (b)(4) highest criticality rating of “High” and yet took anywhere from 4.5 months to over two years to confirm remediation of the vulnerabilities - well beyond the 30 days required by both LifeLock’s policy and the minimum information security standard. In addition, LifeLock maintained inadequate documentation of its remediation efforts.

85. The same is true of LifeLock’s handling of the penetration test vulnerabilities as a whole. LifeLock had not addressed 4 of the penetration test vulnerabilities at all by September 2014, almost two years later. Of the remaining 13 vulnerabilities, only two were addressed in a timely fashion. For every other instance, remediation took over 4 months. In virtually no instance did LifeLock provide sufficient documentation that the issue had been corrected and retested. These failings are symptomatic of a vulnerability remediation process that falls well below the minimum information security standard.

LifeLock Did Not Have a Process for Remediating Vulnerabilities in a Timely Manner

86. LifeLock’s documents show a consistent pattern of remediating vulnerabilities well past the timeframes necessary to meet the minimum security standard. For instance, a LifeLock email dated August 1, 2014, identified a list of 322 VRRs

that were open more than 150 days on August 1, 2014.⁸⁵



Among these are 34 Critical and 107 High VRRs.

87. LifeLock's vulnerability remediation logs also evidence unacceptable delays in correcting vulnerabilities. I reviewed the logs provided by LifeLock covering its VRR tickets generated in the period from April 2012 to May 2015.⁸⁶ At my direction, the FTC prepared for me a statistical analysis of the 1,941 VRR tickets contained in those logs.⁸⁷ I summarize the results of this analysis in Tables 1 to 4 below.

88. The statistical analysis demonstrates that LifeLock did not have a process that resolved vulnerabilities within the timeframes required by the minimum information security standard. The standard requires that all steps in the

⁸⁵ Att. 26, Email from (b)(3):6(f),(b)(4) (Aug. 1, 2014) (LIFELOCK-0134378-385).

⁸⁶ Att. 13.

⁸⁷ Att. 27, Declaration of Elizabeth Anne Miles Pursuant to 28 U.S.C. § 1746 (FTC-0002742-2851) at FTC-0002744-48.

vulnerability remediation process – from discovery of vulnerability to verification of remediation – occur within 30 days for vulnerabilities that LifeLock rates as Critical. Table 1 below shows that LifeLock missed the 30-day timeframe for 133, or 60.5%, of its 220 Critical VRRs. LifeLock’s handling of its Critical VRRs even exceeded the 90 day timeframe for 80 or 36.4% of its 220 Critical VRRs.

Table 1: Analysis of VRRs with Resolution Date Outside 30 and 90 Day Timeframes

VRR Criticality Level	Number of VRRs with Resolution Date Outside 30 Days from Date of Discovery of Vulnerability	Number of VRRs with Resolution Date Outside 90 Days from Date of Discovery of Vulnerability	VRRs with No Dates for Either Resolution or Discovery of Vulnerability	Total Number of VRRs
Critical	<i>133</i>	<i>80</i>	85	220
High	153	109	141	295
Medium	250	112	121	371
Low	516	288	192	708
No Criticality Level Assigned	176	74	167	347
Total	1,228	<i>663</i>	706	1,941

89. The minimum information security standard also requires that LifeLock fully remediate High vulnerabilities within 60 days and Medium/Low vulnerabilities within 90 days. Thus, LifeLock’s ISP cannot meet the standard if its vulnerability remediation process leaves VRRs of any criticality level unaddressed for more than 90 days. Table 1 shows that LifeLock exceeded this 90 day timeframe for 663 or 34.2% of its 1,941 VRRs.

90. LifeLock’s inability to meet the minimum information security standard spanned across most of the period covered by the logs. Table 2 below shows that for 9 out of the 13 quarters covered by the logs, LifeLock failed to meet the 90 day timeframe for at least 20% of its VRRs. In some of the quarters, LifeLock failed to meet the 90 day timeframe for over 50% of its VRRs.

Table 2: Analysis of VRRs with Resolution Date Outside 90 Day Timeframe by Quarter

Quarter	Number of VRRs with Resolution Date Outside 90 Days from Date of Discovery of Vulnerability	VRRs with No Dates for Either Resolution or Discovery of Vulnerability	Total Number of VRRs	Percentage Outside 90 Day Timeframe
2 nd Quarter 2012	73	50	242	30.2%
3 rd Quarter 2012	50	27	213	23.5%
4 th Quarter 2012	74	94	178	41.6%
1 st Quarter 2013	83	20	170	48.8%
2 nd Quarter 2013	119	66	185	64.3%
3 rd Quarter 2013	90	62	156	57.8%
4 th Quarter 2013	53	109	206	25.7%
1 st Quarter 2014	77	49	292	26.4%
2 nd Quarter 2014	32	21	53	60.4%
3 rd Quarter 2014	1	30	32	3.1%
4 th Quarter 2014	2	27	30	6.7%
1 st Quarter 2015	9	129	160	5.6%
2 nd Quarter 2015	0	22	24	0.0%

91. Not only did LifeLock fail to complete all of the remediation steps within the proper timeframes, but in many cases, LifeLock did not even take its first step to address the VRR within those timeframes. The logs indicate the date that LifeLock noted its first action to address a VRR. Table 3 below shows that LifeLock noted its first action for a VRR more than 30 days after discovery of the

vulnerability for 147 or 66.8% of the 220 Critical VRRs. For 47 or 21.4% of the Critical VRRs, LifeLock’s noted its first action more than 90 days after discovery of the vulnerability. For VRRs of all criticality levels, LifeLock noted its first action after the 90 day period for 499 VRRs or 25.7% of the VRRs.

Table 3: Analysis of VRRs with First Action Date Outside 30 and 90 Day Timeframes

VRR Criticality Level	Number of VRRs with First Action Date Outside 30 Days from Date of Discovery of Vulnerability	Number of VRRs with First Action Date Outside 90 Days from Date of Discovery of Vulnerability	VRRs with No Dates for Either First Action or Discovery of Vulnerability	Total Number of VRRs
Critical	<i>147</i>	<i>47</i>	28	220
High	162	107	75	295
Medium	190	73	94	371
Low	410	221	200	708
No Criticality Level Assigned	153	51	139	347
Total	1,062	<i>499</i>	536	1,941

92. LifeLock’s delays in initiating remediation measures were not isolated incidents.

Table 4 below shows that for 5 out of the 13 quarters covered by the logs, the first noted action exceeded the 90 day timeframe for at least 20% of its VRRs. In some

of these quarters, LifeLock exceeded the 90 day timeframe for 50% of its VRRs, including one quarter with 80.1% of its VRRs exceeding the timeframe.⁸⁸

Table 4: Analysis of VRRs with First Action Date Outside 90 Day Timeframe by Quarter

Quarter	Number of VRRs with First Action Date Outside 90 Days from Date of Discovery of Vulnerability	VRRs with No Dates for Either First Action or Discovery of Vulnerability	Total Number of VRRs	Percentage Outside 90 Day Timeframe
2 nd Quarter 2012	38	132	242	15.7%
3 rd Quarter 2012	47	66	213	22.1%
4 th Quarter 2012	91	45	178	51.1%
1 st Quarter 2013	24	44	170	14.1%
2 nd Quarter 2013	98	16	185	53.0%
3 rd Quarter 2013	125	12	156	80.1%
4 th Quarter 2013	50	29	206	24.3%
1 st Quarter 2014	13	64	292	4.5%
2 nd Quarter 2014	1	25	53	1.9%
3 rd Quarter 2014	5	4	32	15.6%
4 th Quarter 2014	2	12	30	6.7%
1 st Quarter 2015	5	74	160	3.1%
2 nd Quarter 2015	0	13	24	0.0%

93. The logs reveal an additional problem with LifeLock’s vulnerability remediation process. An ISP meeting the minimum information security standard must have a formal process to rate the criticality of each vulnerability. However, as shown by Tables 1 and 3, LifeLock’s logs have 347 VRRs (17.9%) with no criticality rating.

⁸⁸ The analysis in Tables 1 through 4 above most likely understates the number of VRRs that LifeLock failed to remediate in a timely fashion for a couple reasons. First, the number of VRRs outside the 30/90 day timeframes cited in the Tables do not include VRRs which are missing their first action dates or resolution dates. Second, as explained in Paragraphs 57 to 63. *supra*, LifeLock downgraded numerous Critical VRRs and most likely addressed them using the longer timeframe for non-Critical VRRs.

Without properly rating each vulnerability, LifeLock has no effective way to ensure that it remediates the more serious vulnerabilities first. In short, from at least April 2012 through March 2014, LifeLock's internal emails and vulnerability remediation logs reveal an ISP that failed to properly categorize and prioritize vulnerabilities and that exhibited significant delays throughout its vulnerability remediation process. These deficiencies rendered LifeLock's vulnerability remediation process incapable of remediating vulnerabilities within the timeframes necessary to meet the minimum information security standard.

LifeLock Lacked a Process for Applying Patches and Updating Outdated Software in a Timely Manner

94. A patch is a software fix issued by a vendor to remediate an exposure or vulnerability in their software. New exposures are found in software on a regular basis. Therefore, an organization should apply available patches to software running on its system on a regular basis. The minimum information security standard requires a formal patching process that identifies, prioritizes, applies, and tests all patches for operating systems and critical applications in a timely manner. A determination of whether an application is critical and the importance of applying a particular patch relative to other patches must be based on a formal policy. The timeframe for patching must be designated based on priority and an implementation plan put in place with proper documentation. If for some reason the patch cannot be applied, a formal exception report must be generated with

appropriate remediation measures put in place. Finally, all patches must be tested prior to system production.

95. When a software vendor releases a patch, both an organization and attackers are placed on notice that there is a method for compromising a system. Therefore, the longer the software goes unpatched, the greater the probability that the system will be compromised. While the *Critical Security Controls* recommends that critical patching be applied within 48 hours,⁸⁹ the minimum information security standard requires that critical patches be applied within 30 days of the patch being released, with other high patches applied within 60 days, and medium to low within 90 days. These timeframes also align with LifeLock's stated patching policy.⁹⁰

96. Organizations must also upgrade outdated software. When software is released it often contains vulnerabilities that have not been discovered. The longer a piece of software is publicly available, the greater the chance that vulnerabilities are discovered. Although patching is one method a vendor uses to fix known vulnerabilities, very often releasing a patch requires too much work, so vendors will release a new version of the software instead. Outdated software has exposures and known methods of compromise. When a new software version is released, vendors often stop supporting the earlier versions. Therefore, failing to upgrade software places an organization at serious risk of an attacker exploiting

⁸⁹ Att. 6, *The Critical Security Controls for Effective Cyber Defense, Version 4.0*, Council on Cyber Security (2012) at FTC-0002275.

⁹⁰ Att. 9, Email from (b)(3);6(f),(b)(4) et al. (July 1, 2013) (LL-0053865-66).

publicly known vulnerabilities in the outdated software. An organization must follow the same protocol for upgrading software as for patching in order to meet the minimum information security standard.

97. The minimum information security standard also requires a consistent process for documenting an organization's patch management activity. The documentation process must identify the available patches and their severity ranking, set timeframes for patching, and log all of the steps taken to deploy the patches. Without consistently documenting such details, an organization will not have the information necessary to keep track of their efforts to timely deploy all required patches.

98. In its September 21, 2012 report, (b)
(3),6 issued a broad recommendation targeting LifeLock's lack of an effective strategy for patching and updating:⁹¹

Track all server software components for security updates. Monitor server software for security advisories and software updates. Develop a strategy to be able to quickly respond to security advisories and integrate security fixes and software updates into production environments. Keeping security fixes and patches up-to-date can avoid exposing serious security holes to attackers and the general public.

99. Among the evidence (b)
(3),6
(4),(b) cited to support its recommendation were 94 Critical or Important Linux patches released from 2007 to 2011 that LifeLock had failed to apply as of September 2012 on just the three servers it examined.⁹²

⁹¹ Att. 28, *Final Report – LifeLock Security Review, Version 1.1*, (b)(3),6(f),(b)(4) (Sept. 21, 2012) (LIFELOCK-2123-181) at LIFELOCK-2130.

⁹² *Id.* at LIFELOCK-2174-77.

Similarly, for just the one Windows server (b)(3):6 (f)(b)(4) examined, (b)(3):6 (f)(b)(4) identified 18 Microsoft patches that had not been applied.⁹³

100. Instead of addressing the long delays in patching, LifeLock downgraded the severity/criticality of patches or mislabeled patches. As the LifeLock information security consultant explained: “This is just not right.”⁹⁴

From: Gwen Ceylon
Sent: Monday, January 07, 2013 7:06 PM
To: Tony Valentine (Tony.Valentine@lifelock.com)
Subject: The thinks that make me shake my head

Check this out. This is one of the metranet sql server database systems. A bunch of Microsoft vulnerabilities – VRR went in as low. But note that the actual risk ranking from the scan engine (which comes from the industry standard Mitre/NIST CVE scores and based on what Microsoft says) is critical and severe. This VRR is a week from being late. They can't just lower the risk ranking to avoid patching systems. Notice also how they lump many vulnerabilities into one VRR – makes it look like vulnerability situation is less than it is when VRR reports are run from service desk. Only 252 open VRRs, but the number of vulnerabilities the 252 VRRs cover is in the 1000's.

This is particularly troublesome when many of the patches (especially for Linux systems) are not only security updates, but also bug fixes to the OS, kernel fixes, etc.... The systems are not getting patched – and the company wonders why there's stability problems?

This is just not right.

101. Despite (b)(3):6 (f)(b)(4) recommendation and the warning from its onsite information security consultant, LifeLock continued to neglect patching. LifeLock provided logs showing Microsoft and Linux patching activity from September 2012 through March 2013.⁹⁵ At my instruction, the FTC ran a statistical analysis on these logs that are summarized in the tables in Paragraphs 102 to 106 below.⁹⁶

⁹³ *Id.* at LIFELOCK-2177.

⁹⁴ Att. 11, Email from Gwen Ceylon to Tony Valentine (Jan. 7, 2013) (LIFELOCK-0038588-89).

⁹⁵ Att. 29, LifeLock's Patching Logs (LIFELOCK-0136812-13, 0138079-80).

⁹⁶ Att. 30, Declaration of Vinayak Balasubramanian Pursuant to 28 U.S.C. § 1746.

102. The analysis shows me that LifeLock consistently missed the timeframes necessary to meet the minimum security standard. For Microsoft patches that Microsoft rated as critical, LifeLock failed to apply 56.6% of them within 30 days:

Microsoft Patch Spreadsheet – Summary Statistics				
	Importance of Patch (Microsoft Ratings)			
	All	Critical	Important	Moderate
Total Number	4755	2290	2421	44
Percent of Whole	100	48.160	50.915	0.9253
Mean	44.387	59.775	29.478	63.909
>30 days (#)	2622	1297	1280	44
>30 days (%)	55.142	56.638	52.871	100
>60 days (#)	884	741	109	36
>60 days (%)	18.591	32.358	4.502	81.818
>90 days (#)	469	403	66	0
>90 days (%)	9.863	17.598	2.726	0

103. The results do not change significantly even if the analysis uses the criticality rating assigned by LifeLock as opposed to Microsoft's criticality rating. Using LifeLock's criticality rating, LifeLock failed to apply 54.4% of the critical patches within 30 days:

Microsoft Patch Spreadsheet – Summary Statistics					
	Importance of Patch (LifeLock Ratings)				
	All	Critical	Important	Med/Moderate	Low
Total Number	4755	2193	2381	53	128
Percent of Whole	100	46.120	50.074	1.115	2.692
Mean	44.387	58.404	28.972	68.679	80.922
>30 days (#)	2622	1193	1247	53	128
>30 days (%)	55.142	54.400	52.373	100	100
>60 days (#)	884	696	91	43	54
>60 days (%)	18.591	31.737	3.822	81.132	42.188
>90 days (#)	469	359	47	9	54
>90 days (%)	9.863	16.370	1.974	16.981	42.188

104. LifeLock’s logs do not show it applying any patches that Linux rates as critical, so I looked at whether LifeLock applied Linux patches of any criticality level within the required 90 day timeframe. The table below shows that LifeLock failed to apply 48% of the Linux patches within 90 days.

‘Linux Patches (no duplicates)’ worksheet – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All	Important	Moderate	Low
Total Number	1141	29	561	551
Percent of Whole	100	2.542	49.167	48.291
Mean	153.787	70.966	177.888	133.608
>30 days (#)	695	20	412	263
>30 days (%)	60.911	68.966	73.440	47.731
>60 days (#)	566	8	369	189
>60 days (%)	49.606	27.586	65.775	34.301
>90 days (#)	548	5	363	180
>90 days (%)	48.028	17.241	64.706	32.668

105. The servers that LifeLock failed to patch in a timely manner included servers in its PCI environment. As shown in the tables below, for the PCI servers, LifeLock failed to apply 55.4% of the critical Microsoft patches within 30 days and 17.4% of the Linux patches within 90 days.

Microsoft Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (Microsoft Ratings)			
	All Data	Critical	Important	Moderate
Total Number	1929	839	1064	26
Percent of Whole	100	43.494	55.158	1.345
Mean	42.900	55.461	32.422	66.385
>30 days (#)	1234	465	743	26
>30 days (%)	63.971	55.423	69.831	100
>60 days (#)	290	229	39	22
>60 days (%)	15.034	27.294	3.665	84.615
>90 days (#)	133	107	26	0
>90 days (%)	6.895	12.753	2.444	0

Linux Patches (no duplicates) (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All Data	Important	Moderate	Low
Total Number	23	8	9	6
Percent of Whole	100	34.783	39.130	26.087
Mean	86.043	82.500	94.778	77.667
>30 days (#)	20	6	8	6
>30 days (%)	86.957	75	88.889	100
>60 days (#)	14	3	5	6
>60 days (%)	60.870	37.5	55.556	100
>90 days (#)	4	2	2	0
>90 days (%)	<i>17.391</i>	25	22.222	0

106. Again, the results do not change significantly for the Microsoft critical patches even if we run the analysis using LifeLock’s own criticality rating. The table below shows that LifeLock failed to apply 50.7% of the Microsoft patches that it rated as critical within the 30 day timeframe.

Microsoft Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics					
	Importance of Patch (LifeLock Ratings)				
	All Data	Critical	Important	Med/Moderate	Low
Total Number	1929	763	1033	33	100
Percent of Whole	100	39.554	53.551	1.711	5.184
>30 days (#)	1234	387	714	33	100
>30 days (%)	63.971	50.721	69.119	100	100
>60 days (#)	290	194	23	29	44
>60 days (%)	15.034	25.426	2.227	87.879	44
>90 days (#)	133	72	10	7	44
>90 days (%)	6.895	9.436	0.968	21.212	44

107. LifeLock’s patching logs, however, only tell part of the story because the logs only cover the patches that LifeLock actually applied and not the universe of patches that LifeLock should have applied. For instance, during the 6 month period covered by the logs, Microsoft released 17 critical operating system

patches.⁹⁷ LifeLock had 17 Windows servers⁹⁸ in its PCI environment and so should have applied 289 patches (17 servers times 17 patches) to these servers. LifeLock's logs show that it only applied 139 of these critical operating system patches to these servers. In addition, LifeLock's logs do not indicate that it applied any critical Linux patches during the 6 month period. In fact, from September 2012 through December 2012, there was only one Linux patch of any criticality level applied to only one of the 189 Linux servers identified by LifeLock.⁹⁹ Given the number of Linux servers in LifeLock's network, it is highly unlikely that none of its servers required a critical Linux patch.

108. LifeLock's own assessment and the PCI assessor's observations confirm my analysis of LifeLock's patching logs.

⁹⁷ The 17 patches and their respective published date are MS12-052 (8/14/12), MS12-054 (8/14/12), MS12-060 (8/14/12), MS12-063 (9/21/12), MS12-071 (11/13/12), MS12-072 (11/13/12), MS12-074 (11/13/12), MS12-075 (11/13/12), MS12-077 (12/11/12), MS12-078 (12/11/12), MS12-081 (12/11/12), MS13-002 (1/8/13), MS13-008(1/14/13), MS13-009 (2/12/13), MS 12-010 (2/12/13), MS13-011 (2/12/13), and MS13-020 (2/12/13). See Microsoft Corporation, *Security Bulletins 2012* (viewed on Jul. 11, 2015) <<https://technet.microsoft.com/en-us/library/security/dn632605.aspx>>.

⁹⁸ The 17 PCI Windows server addresses are REDACTED

See Att. 30.

These 189 servers do not include the 276 decommissioned Linux servers that were active during the relevant time period from September 2012 to March 2014. See Att. 31, Letter from William C. MacLeod, Counsel to LifeLock, Inc., to Susan Pope, Federal Trade Commission (June 12, 2015) (FTC-0002169-2174) at FTC-0002173-74; Att. 32, LifeLock's List of Decommissioned Servers (submitted on Jun. 12, 2015) (LIFELOCK-0138076). LifeLock has stated that it does not have any information regarding whether it applied all of the necessary patches in a timely manner on these decommissioned servers. See Att. 31 at FTC-0002174.

- a. In an internal email, LifeLock acknowledged failing to apply all required Windows and Linux systems patches from approximately December 6, 2012 to March 6, 2013 and explained it was behind “at least by 3 months”:¹⁰⁰

From: (b)(3):6(f),(b)(4)
Sent: Wednesday, March 06, 2013 9:09 AM
To: Rich Stebbins; (b)(3):6(f),(b)(4); Renee Ramirez
Subject: PLEASE READ FOR APPROVAL OR FURTHER DISCUSSION: Vulnerability Remediation and Patch Management -- for PCI Readiness

Importance: High

Good Morning Everyone,

As part of PCI Readiness LifeLock must have a quarterly vulnerability scan and remediate vulnerabilities through system changes or by patching the systems.

For various reasons (ISI for example) patching for Windows and Linux systems have gotten behind, at least by 3 months. PCI requires that High, Medium and Low vulnerabilities be remediated in 30, 60, 90 days respectively. What this means is that LifeLock is behind in remediating most vulnerabilities (all high, most mediums and lows) and the remediation efforts need to be complete in this quarter (by end of March) so that we have a clean scan/remediation to provide to the Auditor.

I have been working with Information Security (Austin) and with key personnel on (b)(3):6 team (Richard and (b)(3):6) to get back into a regular patching / vulnerability remediation cycle. The guys were challenged 2 weeks ago to review the new scans that Austin provided, patches that still need to be applied, and systems that need to be patched and how the systems could be grouped to patched.

- b. As part of the PCI assessment process, in April 2013 the PCI assessor discovered LifeLock’s patching deficiencies when “the Linux team showed the Auditor their Satellite system and specifically (b)(3):6(f),(b)(4) which showed [the assessor] several critical outstanding patches that are months old.”¹⁰¹
- c. The PCI Audit punch list from April 19, 2013 notes: “Main database patches not applies [sic] for some time. Many critical patches over 30 days

¹⁰⁰ Att. 33, Email from (b)(3):6(f),(b)(4) to Rich Stebbins (Mar. 6, 2013) (LIFELOCK-0019638-39).

¹⁰¹ Att. 34, Email from Austin Appel to David Bridgman and (b)(3):6(f),(b)(4) (Apr. 26, 2013) (LIFELOCK-0053824-25) at LIFELOCK-0053825.

old. Patch classification downgraded without documented justification.”¹⁰²

(Emphasis added).

109. Because LifeLock arbitrarily downgraded the criticality rating of the patches, the analysis in tables in Paragraphs 102 to 106 above understates the number of critical patches that LifeLock failed to deploy within the lowest acceptable timeframe.
110. Moreover, arbitrarily downgrading the criticality rating of patches independently falls below the minimum information security standards. An organization cannot consistently deploy patches on a timely basis without accurate information regarding the criticality of their patches.
111. A major part of the reason that LifeLock missed so many patches was because it failed to maintain an operational patch deployment system and properly document its patching. LifeLock used (b)(3);6(f),(b)(4) (b)(3);6(f),(b)(4) and Windows Server Update Services (WSUS), to deploy patches.¹⁰³ However, in November 2012, (b)(3);6(f),
(b)(4) and WSUS [were] both broke” and LifeLock’s “Windows team refuse[d] to patch systems

¹⁰² Att. 35, LifeLock, Inc. PCI Audit Punch List (Apr 19, 2013) (LIFELOCK-0009259-61) at LIFELOCK-0009260.

¹⁰³ Att. 36, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Federal Trade Commission, (Jan. 2, 2015) (LIFELOCK-0134224-40) at LIFELOCK-0134231.

manually...” The result was that “vulnerabilities [were] increasing in number putting the company at greater risk,”¹⁰⁴ a fact confirmed by the patch analysis.

112. It appears LifeLock did not begin to resolve this issue until late-May 2013, over six months later.¹⁰⁵ In my opinion, LifeLock should have identified this issue within 30 days of it first arising and resolved it within two to three months. The failure to systematically deploy patches to remediate vulnerabilities for at least 7 months falls below minimum information security program standards.

113. Problems with LifeLock’s patch deployment system resurfaced in November 2014 when technical problems with (b)(3);6(f), (b)(4) WSUS and (b)(3);6(f),(b)(4) (b)(3);6(f),(b)(4) prevented LifeLock from using the system to apply Adobe Flash updates/patches.¹⁰⁶

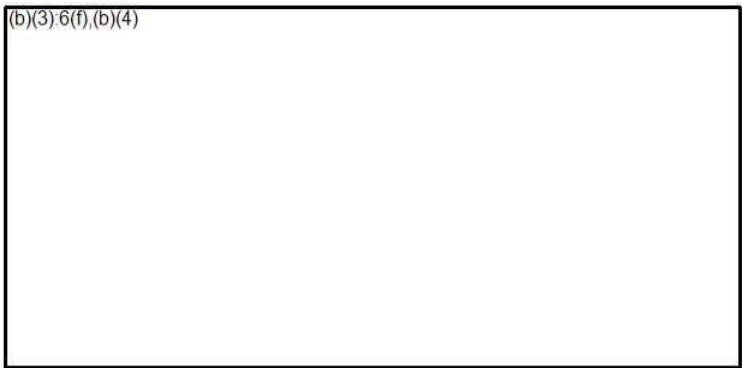
114. LifeLock’s lack of an effective patch management process created serious vulnerabilities by leaving Windows and Linux systems exposed for significant periods of time. A patch fixes a known point of exploitation so failing to patch greatly increases the risk of exposure and is unacceptable from a security perspective. In addition to unpatched Windows and Linux systems, (b)(3);6(f), (b)(4) warned that “[m]ultiple instances of outdated software were identified. These outdated systems could contain a number of flaws which could be exploited to

¹⁰⁴ Att. 37, Email from Jenner Holden to Gwen Ceylon (Nov. 16, 2012) (LIFELOCK-0088187-88) at LIFELOCK-0088187.

¹⁰⁵ Att. 38, LifeLock PowerPoint Presentation, *Q2-Implement Monitoring Phase I Project (AP)* (2013) (LIFELOCK-0077845) at 10.

¹⁰⁶ See *infra* ¶ 165.

compromise the system or deny service to legitimate users.”¹⁰⁷ For example, LifeLock’s Tomcat application was out of date by at least one year and contained “numerous vulnerabilities”.¹⁰⁸



115. Tomcat is software that runs websites. Websites are the front end interface to back end databases that store critical information. Having access to a web server provides an easy way for an adversary to compromise sensitive information. At least one internal document suggests this was a “false positive” penetration test finding¹⁰⁹ and thus it was never formally addressed as a response to a penetration test vulnerability. LifeLock’s vulnerability logs, however, make clear it was not a false/positive and the vulnerability was even greater than what the penetration test identified.

¹⁰⁷ Att. 15, *LifeLock, Inc.: Information Assurance Services Enterprise Security Assessment*, (b)(3):6(f),(b)(4) (Nov. 13, 2012) (LIFELOCK-0053403-61) at LIFELOCK-0053408-09.

¹⁰⁸ *Id.* at LIFELOCK-0053423.

¹⁰⁹ Att. 18, *LifeLock’s Documentation of Penetration Test Vulnerability Remediation* Submitted to (b)(3):6(f),(b)(4) (submitted Jul. 2013) (LIFELOCK-00132479-516) at LIFELOCK-132486.

116. According to the vulnerability remediation management logs, two months after the penetration test, January 15, 2013, a VRR ticket was created explaining:

During the network pen test the pen testers [sic] found that the installed version of tomcat on (b)(3);6(f),(b)(4) has numerous [sic] vulnerabilities including multiple denial of service bugs, multiple XSS vulnerabilities and other significant vulnerabilities. While the pen testers scanner detected version 5.5.30 installed according to the banner, this server is actually running version 5.5.23 which has even more vulnerabilities.

(Emphasis supplied).¹¹⁰ The VRR ticket details 36 vulnerabilities with the Tomcat version LifeLock was then using.¹¹¹ The publish date for these vulnerabilities dated from June 14, 2007 to November 30, 2012, with 27 of these vulnerabilities published prior to 2012.¹¹²

117. Although these vulnerabilities were identified in the November 13, 2012 penetration test, no VRR ticket was apparently created until January 15, 2013. The Tomcat web server application was apparently not updated for almost three more months. On April 2, 2013, a note in the log indicates that LifeLock

“[u]pgraded the system to the latest version and for this server the latest (b)(3);6(f),(b)(4)

¹¹⁰ Att. 13, LifeLock’s VRR Logs (322 Open Requests WO Tables with Notes, generated by (b)(3);6(f),(b)(4) (May 27, 2015); VRRs – June 2012 to September 2012 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – October 2012 to March 2013 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – April 2013 to December 2014 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – April 2012 to May 2015 ARC Table with Notes, generated by (b)(3);6(f),(b)(4) (May 29, 2015); VRRs – April 2012 to May 2015 WO Table with Notes and Priority, generated by (b)(3);6(f),(b)(4) (May 29, 2015) (LIFELOCK-0135783-86, 0138077-78) at LIFELOCK-0135783 (line 143).

¹¹¹ Att. 39, Email from (b)(3);6(f),(b)(4) to Austin Appel (April 03, 2013) (LIFELOCK-0033129-33).

¹¹² *Id.*

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

LifeLock did not close this request until April 22, 2015, without any explanation beyond a “N/A” designation. Thus, which Tomcat version is currently in use is unclear as is the status of vulnerabilities from the outdated software.¹¹³

118. LifeLock’s Tumbleweed is another example of LifeLock’s deficient patch management process creating vulnerabilities in critical software. Tumbleweed is software that provides a method for transferring sensitive files in a secure manner. Tumbleweed vulnerabilities provide an easy gateway for an adversary to compromise these sensitive files.

119. In October 2013, LifeLock’s Security Engineer, Andrew Citro, explained, “We are –WAY—out of date on updating Tumbleweed, and have been even when I first started.”¹¹⁴ (Emphasis original.) Mr. Citro identified two vulnerabilities resulting from the outdated Tumbleweed, one dating from 2003 and another dating from 2011, but he could not upgrade the software to resolve the vulnerability as the software was too outdated.¹¹⁵ Apache, which is the web server that is used by Tumbleweed, had exposures that would allow someone to access sensitive information and/or perform a denial of service attack to make the system unavailable. Since Tumbleweed was out of date, Apache could not be updated and the exposures could not be remediated. Further, the software

¹¹³ Att. 13 at LIFELOCK-0135783 (line 143).

¹¹⁴ Att. 40, LifeLock, Security Exception Risk Assessment Form (June 30, 2014) (LIFELOCK-0034400-01) at LIFELOCK-0034400.

¹¹⁵ *Id.*

version was so out-of-date that the vendor did “not have patches for the version of tumbleweed that [LifeLock was] running.”¹¹⁶

120. Although the identified vulnerabilities had existed since 2003 and 2011 respectively, LifeLock did not seek a “Security Exception” to continue running the software with this vulnerability in place until October 2013.¹¹⁷ Because LifeLock had “no plan to upgrade Tumbleweed,” the proposed resolution in October 2013 was to “mitigate the risk by encrypting the fields as they traverse Tumbleweed.”¹¹⁸
121. Over four months later, in late-February 2014, LifeLock concluded that it could resolve one of the vulnerabilities after all and did so. The other vulnerability was granted a security exception with the mitigating control of “encrypting the fields with the information as they traverse Tumbleweed.”¹¹⁹
122. LifeLock’s patch management process also did not have sufficient documentation to support the gaps in the patching that existed. The analysis of the patch logs shows that the patches were not applied consistently across all servers, and for a given server, not all of the applicable patches were applied. If a patch is not applied, LifeLock should have had in place a formal process for verifying and documenting that the lack of a patch did not create a security exposure.

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *Id.*

123. Problems with its patch deployment software, insufficient documentation, and other technical and non-technical reasons likely contributed to LifeLock's patch management failures. In any event, from at least September 2012 to March 2013, LifeLock consistently failed to deploy critical patches within 30 days and all patches within 90 days. Accordingly, LifeLock's ISP did not have an effective patching process necessary to meet the minimum information security standard for at least that time period.

LifeLock Did Not Have Effective Processes for Configuration Management and Password Management

124. Changes in the network, such as the installation of new software or patches, could create vulnerabilities if not properly managed. New software introduces new services which may serve as additional avenues for an attacker to gain unauthorized access into the network. New software may also have default parameters set up by the vendor for installation convenience and that are known by all purchasers of the software. Leaving these default parameters in place would make unauthorized access to the system more likely. Also, patches remediate vulnerabilities in the patched software but could cause unexpected vulnerabilities elsewhere in the network that an attacker could exploit.

125. For these reasons, the minimum information security standard requires an organization to implement all system changes through a formal change management process to ensure that the changes are secure and do not degrade the security of the system. A change management process mitigates this risk

through system hardening, which involves configuring software in the system to reduce exposure points introduced by the system change. For instance, system hardening would remove unnecessary services or change the default parameters in new software. An effective change management process also tests the change and scans the system for vulnerabilities prior to putting the change into production. All of these steps require thorough documentation so that the organization can track and verify its change management efforts.

126. In addition, the minimum information security standard requires an organization to manage password access to network resources so that employees' use of weak passwords does not compromise an otherwise well-configured network. User credentials, which include a user name and a password, allow system access. If a password is easy to guess, or the same password is used for multiple systems, it provides the opportunity for an adversary to gain access to a system and compromise sensitive client information. In particular, administrative or manager credentials are extremely sensitive because if compromised they allow an attacker (either internal or external) wider system access. Manager credentials can provide full access to a system, including the ability to read, change, or delete information.
127. An organization must have a process for ensuring that employee passwords are unique, properly protected, and only available to those needing account access. Passwords must also be periodically changed to minimize or reduce the chance

of compromise. An organization must also monitor account credentials (which include passwords) for any adverse activity or signs of an attack.

128. Both the Nov. 2012 (b)(3):6(f),
(b)(4) and Sept. 2012 (b)(3):6
(f),(b)(4) security assessments noted serious deficiencies in LifeLock’s configuration management. (b)(3):6
(f),(b)(4) identified 9 configuration management vulnerabilities, 8 of which it rated “High” or “Medium” severity.¹²⁰ (b)(3):6(f),
(b)(4) identified two “High” and 7 “Medium” severity configuration management vulnerabilities as indicated in the figure below.¹²¹

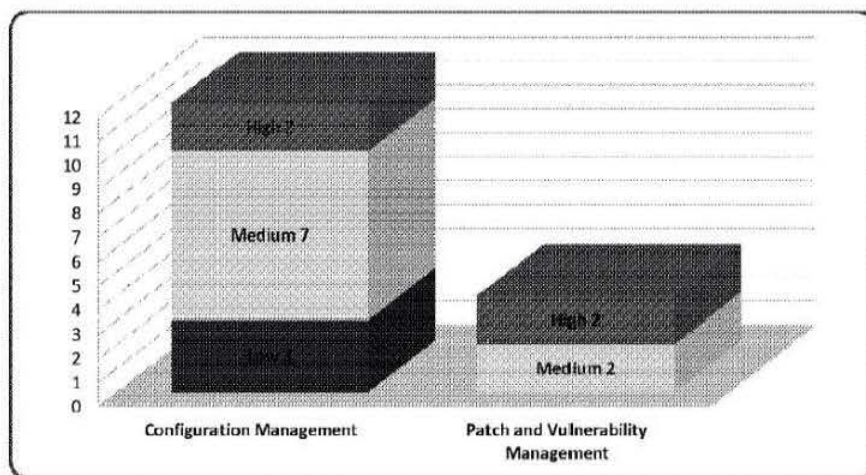


Figure 1: Vulnerability Summary – By Root Cause and Severity Level

¹²⁰ Att. 28, *Final Report – LifeLock Security Review, Version 1.1*, (b)(3):6(f),(b)(4) (Sept. 21, 2012) (LIFELOCK-2123-81) at LIFELOCK-2137. (b)(3):6
(f),(b)(4) describes a “Medium” severity vulnerability as “[i]ndividual user’s information is at risk, exploitation would be bad for client’s reputation, moderate financial impact or possible legal implications for client.” It describes a “High” severity vulnerability as “[l]arge number of users, very bad for client’s reputation or serious legal and or financial implications.” *Id.* at LIFELOCK-2135.

¹²¹ Att. 15, *LifeLock, Inc.: Information Assurance Services Enterprise Security Assessment*, (b)(3):6(f),(b)(4) (Nov. 13, 2012) (LIFELOCK-0053403-61) at LIFELOCK-0053409. (b)(3):6(f),
(b)(4) describes a “Medium” severity vulnerability as causing “[t]angible impact; potential damage to data and resources” and a “High” severity vulnerability as causing “[s]ignificant impact; probable damage to data and resources.” *Id.* at LIFELOCK-0053447.

129. (b)(3):6(f), (b)(4) “observed default or insecure configuration standards throughout the infrastructure.”¹²² For example, SMB Null Sessions, SNMP Default Community Strings, and clear text protocols are all vulnerabilities associated with the use of default installations.¹²³ I would also include Directory Traversal vulnerability as a default installation problem.¹²⁴ These are all well-known vulnerabilities that a configuration management process meeting the minimum information security standard would have prevented. Accordingly, (b)(3):6(f), (b)(4) offered recommendations aimed at correcting basic deficiencies in LifeLock’s configuration management process:

- “LifeLock should review the change and configuration management procedures to ensure that system hardening is integrated into each step of the change management process.”
- (b)(3):6(f),(b)(4) also recommends that regular vulnerability assessments be performed on the internal network to quickly identify outdated or misconfigured systems.”¹²⁵

130. LifeLock’s internal documents confirm (b)(3):6(f),(b)(4) findings regarding LifeLock’s configuration management deficiencies. On May 13, 2013, LifeLock identified as a goal “Create/Implement Database Auditing and Database Security Standards

¹²² *Id.* at 0053449.

¹²³ *Id.* at LIFELOCK-0053424, 0053426, 0053429.

¹²⁴ *Id.* at LIFELOCK-0053421. Default installation or misconfiguration of the system are the only methods by which a Directory Traversal vulnerability could have occurred. Given LifeLock’s practices, it is more likely this occurred due to a default installation. As explained earlier, a Directory Traversal vulnerability allows bypassing of access controls, allowing an attacker access to system information, including sensitive files.

(b)(3):6(f), (b)(4) exploited the Directory Traversal vulnerability to gain control of the (b)(3):6(f),(b)(4) domain. *See infra* ¶¶ 74-77.

¹²⁵ Att. 15 at LIFELOCK-0053409.

and Procedures, and Database Hardening Standards and Procedures” by the third and fourth quarter of 2013.¹²⁶ More than three months later, LifeLock was still in the process of hardening and securing its databases, and developing security and hardening procedures. In late August, LifeLock charted its progress as:

- Implement Database Security Standards – 50% complete;
- Implement Database Hardening Standards – 50% complete;
- Update Database Security Standards and Procedures – 25% complete;
- Update Database Hardening Standards and Procedures – 25% complete.¹²⁷

According to LifeLock’s documents, as of late August 2013, LifeLock had not put in place the system security and hardening that are basic elements of a configuration management process.

131. LifeLock also lacked an effective change management process in 2012 and 2013. In November 2012, LifeLock’s information security consultant warned, “well defined change management plan not in place, people are not following the process.”¹²⁸

132. Four months later, in an email exchange between LifeLock’s information security consultant, (b)(3)-6(f),(b)(4) and its Senior Director for Infrastructure,

¹²⁶ Att. 41, Email from Loretta Stagnitto to Rich Stebbins (May 13, 2013) (LIFELOCK-0023835-36) at LIFELOCK-0023836 (pg. 11).

¹²⁷ Att. 42, Email from Andy Doyle to Rich Stebbins (Sep. 30, 2013) (LIFELOCK-0077495-96) at LIFELOCK-0077496 (pg. 5).

¹²⁸ Att. 37, Email from Jenner Holden to Gwen Ceylon (Nov. 16, 2012) (LIFELOCK-0088187-88) at LIFELOCK-0088187.

(b)(3):6(f),(b)(4) LifeLock acknowledged serious gaps in the change management process:

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

(Emphasis supplied).¹²⁹ LifeLock’s change management process apparently had no consistent scanning and was not even “fully documented and... vetted...”

133. Approximately two months later, in May 2013, LifeLock’s PCI assessor found that “LifeLock is not performing security scans before major system or code changes are released into the CDE environment.”¹³⁰ Even in late July 2013, the lack of consistent scanning remained a problem. A LifeLock internal email states that “one thing LL is really lacking is having significant changes scanned after they go into production.”¹³¹

134. In short, LifeLock did not appear to have any formalized process for configuration management. At least as of March 2013, LifeLock did not have a

¹²⁹ Att. 43, Email from (b)(3):6(f),(b)(4) to Scott Watson *et al.* (Mar. 19, 2013) (LIFELOCK-0026183-84) at LIFELOCK-0026183.

¹³⁰ Att. 44, *PCI DSS Gap Analysis Report*, (b)(3):6(f),(b)(4) (May 21, 2013) (LIFELOCK-0095891-959) at LIFELOCK-0095896.

¹³¹ Att. 45, Email from (b)(3):6(f),(b)(4) to AnneMarie Olson and Austin Appel (Jul. 25, 2013) (LIFELOCK-0029627-28) at LIFELOCK-0029627.

“fully documented and... vetted” configuration management process in place, and even as late as August 2013, it lacked hardening procedures for its database. To the extent LifeLock did have a process, “people [were] not following the process,” and the process lacked a critical component – the consistent scanning of system changes. For these reasons, LifeLock’s configuration management process did not meet the minimum information security standard in 2012 and 2013. LifeLock’s password management process also fell below the minimum information security standard. Both (b)(3);6(f) and (b)(3);6(f), (b)(4) identified LifeLock’s failure to properly manage Local Administrator passwords as a significant vulnerability. (b)(3);6(f), (b)(4) found that LifeLock utilized “passwords that never expired” for its Windows and Linux hosts, and that it used the same password across hosts on each platform. Accordingly, (b)(3);6(f), (b)(4) security assessment report recommended that LifeLock implement basic password management protocols:¹³²

Change the passwords for local Root and Administrator accounts. Apply this across the environment and ensure that they are also changed every 90 days. Also change the (b)(3);6(f), (b)(4) root account password on the (b)(3);6(f), (b)(4)

135. (b)(3);6(f), (b)(4) confirmed that LifeLock’s password management failures were widespread as “local administrator credentials were verified as being reused throughout the enterprise.”¹³³

¹³² Att. 28 at LIFELOCK-2129.

¹³³ Att. 15, *LifeLock, Inc.: Information Assurance Services Enterprise Security Assessment*, (b)(3);6(f), (b)(4) (Nov. 13, 2012) (LIFELOCK-0053403-61) at LIFELOCK-0053422.

136. The risk posed by LifeLock’s password management practices is demonstrated by the successful attack (b)(3):6(f),
(b)(4) launched as part of its penetration test. In the attack, “the reuse of local administrator passwords ultimately enabled the compromise of the domain.”¹³⁴ LifeLock admitted this gave (b)(3):6(f),
(b)(4) domain administrator rights which is “‘superuser’ access to a domain and is the highest level of access that a user can have.”¹³⁵ LifeLock explained:

(b)(3):6(f),
(b)(4) was able to create a user with domain admin rights. With domain admin rights, one has full access (or the ability to give oneself full access) to any Windows system joined to the domain, any file share or other systems connected to the Active Directory.¹³⁶

The domain admin rights allowed access to the LifeLock database containing “member billing information”¹³⁷ and to the (b)(3):6(f),(b)(4) application “[u]sed by Member Service agents to review members’ accounts.”¹³⁸ Knowing this one password allowed (b)(3):6(f),
(b)(4) administrative access to any other system across the organization that used the same password.

137. Although (b)(3):6(f),
(b)(4) identified the password vulnerability to LifeLock in its November 13, 2012 report, it took more than 4 months before LifeLock

¹³⁴ *Id.* at LIFELOCK-0053437. This highlights a discrepancy in the PCI Assessment. The PCI Assessment claims LifeLock passed the PCI DSS requirement for passwords, but other assessments show that LifeLock was deficient in this area.

¹³⁵ Att. 46, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Federal Trade Commission (Dec. 9, 2014) (LIFELOCK-0134215-16) at LIFELOCK-0134215.

¹³⁶ Att. 47, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Federal Trade Commission (Dec. 3, 2014) (LIFELOCK-134056-65) at LIFELOCK-0134060.

¹³⁷ *Id.* at LIFELOCK-0134061.

¹³⁸ *Id.* at LIFELOCK-0134065

addressed this High severity vulnerability that (b)(3):6(f),
(b)(4) exploited to gain “superuser” access to the domain.

138. (b)(3):6(f),
(b)(4) launched a second successful attack as part of the penetration test by exploiting another password vulnerability. The attack took advantage of LifeLock’s Apache Tomcat installations which had multiple “easily guessable administrative credentials of manger/manger.”¹³⁹ Having such a guessable manager credentials means an internal or external attacker could easily figure out the password, login as a manager, and gain extensive access to the system. Once again, poor credential management at the administrator level enabled a successful attack. And here too, it was over 4 months before LifeLock resolved this vulnerability.

139. If LifeLock had a functioning process for managing passwords, it would have either prevented these password vulnerabilities, or at the very least, remediated these vulnerabilities much earlier than the 4 months that it took. The basic level and the pervasiveness of LifeLock’s problem with insecure local administrator credentials demonstrate that it lacked a password management process that meets minimum information security standards.

LifeLock Did Not Have an Effective Process for Documenting Critical Information in Its Database Monitoring and Activity Logs

140. To meet the minimum information security standard, an organization must monitor its network for intrusions. If an organization does not monitor, it will

¹³⁹ Att. 15 at LIFELOCK-0053437.

not be able to stop or mitigate an attack in a timely manner. An organization must also monitor its vulnerability remediation, patching, and configuration and password management processes to ensure that they are running properly.

141. An organization cannot effectively monitor without logs that cover each of these processes. For instance, logs feed the alerting system for intrusions, and logs provide the information necessary to plan next steps of a remediation. Without logs, an organization is blind to what is happening on their system and cannot tell if an incident has occurred or a necessary system repair has taken place.
142. Because of the importance of these logs, the minimum information security standard requires a process for consistently documenting all of the relevant activities.
143. An organization must also archive its logs. Attacks are often not detected immediately, and an organization needs the ability to reconstruct a past attack and the condition of the network at the time using archived logs.
144. LifeLock's logging falls below the minimum information security standard. On multiple occasions, LifeLock failed to provide logs that the FTC requested and that LifeLock should have maintained. The FTC requested that LifeLock produce the logs from its security incident and event management (SIEM) alerting tool (b)(3);6(f),(b)(4) used to monitor, identify, and detect potential security threats and incidents. LifeLock could not use the logs to reproduce the (b)(3);6(f),
(b)(4)

results. LifeLock claimed that their SIEM tool had analyzed all of the logs, but it was unable to process the logs through the SIEM tool to verify its claim.¹⁴⁰

145. The FTC also requested the production of logs reflecting the Microsoft and Linux patch histories on LifeLock’s servers for September 2012 through March 2013. In response, LifeLock had one of its engineers create a script to “conduct an automated pull of patch history directly from these machines.”¹⁴¹ It appears that LifeLock did not maintain a central and readily accessible log of its patching activity.

146. Moreover, LifeLock was unable to produce any Microsoft and Linux patch history logs for servers that are currently decommissioned but were in operation during the September 2012 through March 2013 timeframe.¹⁴² LifeLock is thus unable to document any of the Microsoft or Linux patching that took place on these servers for that time period.¹⁴³

147. In my experience, LifeLock’s failure to maintain its (b)(3)6(f),
(b)(4) and patching logs represents a significant deficiency because the logs give an organization vital

¹⁴⁰ LifeLock’s deficient logging practices could explain the fact that LifeLock identified only 4 security breaches or incidents related to LifeLock’s ISP from October 2012 to December 2014. *See* Att. 46 at LIFELOCK-134216; Att. 48, LifeLock Response to FTC 3/13/14 Information Request (Apr. 15, 2014) (LIFELOCK-3166-74) at LIFELOCK-3173. An organization of LifeLock’s size and with the type of information it retains would be targeted on a much more frequent basis. Similarly sized organizations with proper detection systems identify incidents at least monthly, if not weekly.

¹⁴¹ Att. 31, Letter from William C. MacLeod, Counsel to LifeLock, Inc., to Susan Pope, Federal Trade Commission (Jun. 12, 2015) (FTC-0002169-2174) at FTC-0002172.

¹⁴² *Id.* at FTC-0002174.

¹⁴³ As noted in Paragraph 108, this is a timeframe when LifeLock was “at least” 90 days behind in applying Windows and Linux patches.

information regarding the security state of its network. Without these logs, LifeLock did not have sufficient information to properly track security incidents and the progress of its patching activities. In short, LifeLock lacked a monitoring and logging process that met the minimum information security standard.

LifeLock’s PCI Assessment and Certification

148. LifeLock obtains annual Payment Card Industry Digital Security Standard (PCI DSS) Attestation of Compliance (PCI AOC) as required by the major credit card companies for vendors to process credit card payments from their customers. LifeLock’s PCI AOCs, however, do not prove that it had an ISP meeting minimum information security industry standards. The PCI AOC is a point-in-time assessment and does not indicate an ongoing commitment to security. More importantly, the LifeLock documents I reviewed show that LifeLock should never have received its PCI AOC, at least in 2013. LifeLock did not meet PCI DSS for significant periods in 2012, 2013, and 2014, and missed specific PCI requirements in its 2013 PCI assessment.

PCI AOC Does Not Demonstrate On-Going Compliance

149. LifeLock’s PCI AOC does not demonstrate that LifeLock is continually maintaining an ISP that meets the requirements of the Order. The information security industry distinguishes between *validation*, which is “a point-in-time event . . . that attempts to measure and describe the level of adherence to the standard,” and *compliance*, which is “a continuous process of adhering to the

regulatory standard.”¹⁴⁴ A PCI AOC is a point-in-time validation regarding the state of LifeLock’s ISP at the time of the assessment – not proof of compliance as required by the Order.¹⁴⁵

150. Many organizations that have had security breaches may have been previously adjudged PCI compliant at the time of the assessment but did not maintain compliance with PCI standards at the time of the breach. According to Bob Russo, General Manager Emeritus at PCI Security Standards Council:

It’s been our experience that none of the breaches that occurred have been compliant at the time of the breach. Becoming compliant with the standard is pretty much a snapshot in time. An assessment company would come in and go through all those requirements and check that this stuff is in place. If everything is in place they issue a report on compliance. It is then your responsibility as a merchant to maintain that compliance.¹⁴⁶

151. Some organizations, including LifeLock based on my review, focus on simply passing a PCI assessment. However, after the PCI assessors complete their yearly assessment, they do not maintain their information security.

LifeLock’s July 2013 PCI AOC Was Not Warranted

152. LifeLock should not have received its PCI AOC in July 2013 because it did not meet all of the requirements for certification. In order to receive certification,

¹⁴⁴ Att. 49, C. Valladares, *PCI DSS Compliance: More Carrot and Less Stick?*, Tripwire.com (May 17, 2011) (FTC-0002852-60) at FTC-0002852-53. Tripwire is an industry leader in cybersecurity products.

¹⁴⁵ My explanation of how the 2012 assessments by (b)(3);6 (f),(b) and (b)(3);6(f), (b)(4) differ in scope from the Order’s requirement for a comprehensive ISP applies with equal force to this discussion. See *supra* ¶¶43-47.

¹⁴⁶ Att. 50, E. Mills, *PCI compliance: What it is and why it matters (Q&A)*, CNET.com (Feb. 8, 2010) (FTC-0002861-69) at FTC-0002863.

LifeLock's PCI assessor, (b) (3)(6)(f) required LifeLock to demonstrate that it remediated the vulnerabilities identified by the penetration tests in late 2012. Although LifeLock was able to persuade (b) (3)(6) that it had "corrected and retested" those vulnerabilities, as explained above, the evidence demonstrates otherwise.¹⁴⁷ LifeLock's documents submitted to (b) (3)(6) do *not* show that it remediated the penetration test vulnerabilities as of the assessment date, and LifeLock conceded that a number of vulnerabilities remained unremediated even as late as September 2014.

153. In addition, in order to be PCI compliant all VLANs that contain cardholder data must be included within the scope of the report and scanned at least quarterly.¹⁴⁸ Scanning all of the servers in the PCI environment is essential to system security because an attacker can exploit vulnerabilities on one server to access other servers in the system. Internals emails, however, show that not all PCI VLANs were in fact being scanned. In late March 2013, LifeLock's information security staff discovered that they had failed to include certain VLANs containing cardholder data in LifeLock's PCI scans but were "not prepared to declare that to the [PCI] Auditor."¹⁴⁹ Later, on July 15, 2013, just days before the PCI certification was due, LifeLock's information security consultant told LifeLock's

¹⁴⁷ See *supra* ¶¶ 64-85.

¹⁴⁸ Att. 7, *Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, v. 2.0*, PCI Security Standards Council (Oct. 2010) (FTC-0002094-2168) at FTC000-2100, 2153.

¹⁴⁹ Att. 51, Email from Austin Appel to David Bridgman (Mar. 25, 2013) (LIFELOCK-24609-10) at LIFELOCK-24609.

internal auditor that LifeLock could not satisfy the PCI scanning requirement:¹⁵⁰

From: (b)(3)-6(f),(b)(4)
Sent: Monday, July 15, 2013 12:12 PM
To: Tony Valentine
Subject: FW: ROC - Updated list of Critical and Post-ROC Items - Version 3
Importance: High

Tony,

Austin is able to do a screenshot of all scans run and dates that they ran. BUT – some of these scans were added after I came in because I had noticed (along with (b)(4)) that not all PCI vlans were being scanned.

Now this is going to be noticed by (b)(4) because not all vlans have a year's worth of scans when they should have (b)(3)-6(f),(b)(4)

(b)(4) alternative request (DMZ and CDE)...DMZ would be fine but the CDE I think means all the CDE vlans (which is all we scan anyway, and doesn't mean we can remove those vlans that have not been scanned all year)

THOUGHTS?

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

154. In September 2014, LifeLock confirmed to the FTC that it had not conducted quarterly scans on all in-scope PCI VLANs.¹⁵¹ This shows that LifeLock's PCI RoC incorrectly states that LifeLock complied with PCI Requirement 11.2.1 and

¹⁵⁰ Att. 52, Email from Tony Valentine to (b)(3)-6(f),(b)(4) (Jul. 15, 2013) (LIFELOCK-0010367-74) at LIFELOCK-0010367.

¹⁵¹ Att. 21, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Attorney, Federal Trade Commission (Sept. 19, 2014) (LIFELOCK-0110772-81) at LIFELOCK-0110780.

that LifeLock should not have passed its PCI assessment:¹⁵²

<p>11.2.1 Perform quarterly internal vulnerability scans.</p>	<p>11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.</p>	<p>Yes</p>	<p>TVS interviewed Austin Appel, Information Security Analyst I, and determined that vulnerability management processes exist. Austin Appel indicated that internal vulnerability scanning with (b)(3):6(f),(b)(4) is performed (b)(3):6(f),(b)(4) reviewed scan reports that are created and stored during (b)(3):6(f),(b)(4) for the last 12 months. PCI (4th St Voice) 10.30.192.0.PNG, PCI (Application) 10.10.11.0.PNG, PCI (Authentication) 10.10.51.0.PNG, PCI (Citrix) 10.10.56.0.PNG, PCI (Database)</p>
---	--	------------	---

155. Likewise, LifeLock failed to meet PCI Requirements 6.1 and 6.2. PCI Requirement 6.1 requires the installation of vendor supplied critical security patches “within one month of release.”¹⁵³ As detailed above at Paragraph 105, from September 2012 through March 2013, LifeLock’s average time for installing critical Microsoft patches in its PCI environment was 55.5 days, with 55.4% of the critical patches taking more than 30 days to patch and almost 27.3% taking longer than 60 days. LifeLock also did not install a single critical Linux patch even though it likely would have had several hundred given the size of its network.
156. PCI Requirement 6.2 states that an organization must “[e]stablish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.”¹⁵⁴ LifeLock failed to meet this requirement by unilaterally downgrading the rankings of critical patches and vulnerabilities.¹⁵⁵

¹⁵² Att. 17, PCI Report on Compliance for LifeLock, (b)(3):6(f),(b)(4) (Jul. 2013) (LIFELOCK-0097021-229) at LIFELOCK-0097199.

¹⁵³ Att. 7 at FTC-0002131.

¹⁵⁴ *Id.* at 39. PCI DSS gives guidance for a ranking policy by providing the following example: “criteria for ranking ‘High’ risk vulnerabilities may include a CVSS base score

157. Because LifeLock did not meet these PCI requirements, it should not have received an unqualified PCI certification.

LifeLock Did Not Have a PCI Compliant ISP in 2012, 2013, and 2014

158. July 2013 was not the only time that LifeLock did not have a PCI compliant ISP. LifeLock’s ISP did not meet PCI DSS for significant periods in 2012, 2013, and 2014 because of the deficiencies, as detailed in this Report, in LifeLock’s vulnerability remediation management, patching processes, configuration management, and password management.¹⁵⁶ Among other violations, LifeLock did not “[a]lways change vendor-supplied defaults before installing a system on the network” (PCI Requirement 2.1), “[e]nsure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software” (PCI Requirement 5.1.1), “[i]nstall critical security patches within one month of release” (PCI Requirement 6.1), “[f]ollow change control processes and procedures” (PCI Requirement 6.4), and enforce unique password requirements (PCI Requirement 8.2).¹⁵⁷

159. Numerous LifeLock documents demonstrate its lack of continuous PCI compliance. For instance, a January 20, 2013 report identifies a Security

of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as ‘critical,’ and/or a vulnerability affecting a critical system component.” *Id.*

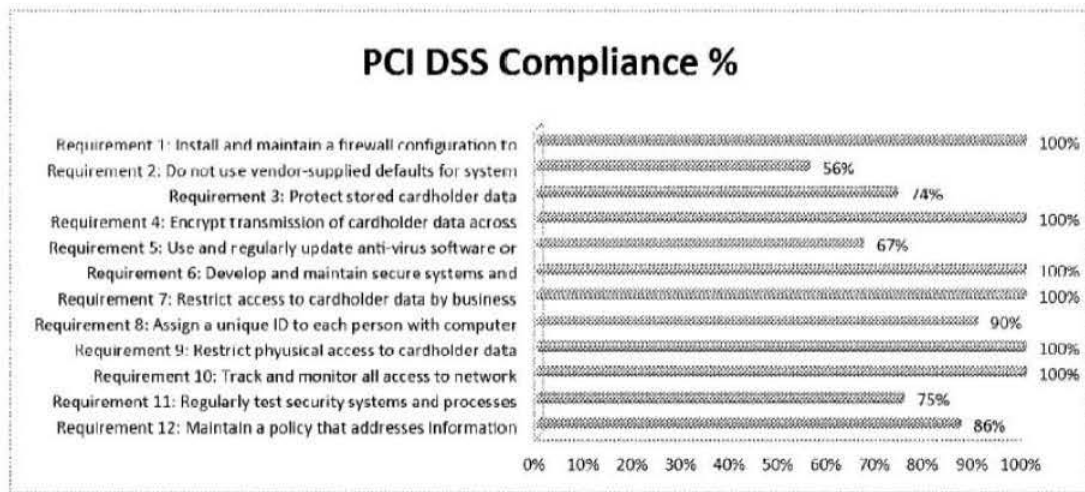
¹⁵⁵ See *supra* ¶¶ 57-63, 108.

¹⁵⁶ PCI DSS is a higher standard than the lowest acceptable security standard that LifeLock failed to meet by exhibiting these ISP deficiencies.

¹⁵⁷ Att. 7, *Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, v. 2.0*, PCI Security Standards Council (Oct. 2010) (FTC-0002094-2168) at FTC-0002117, 0002130, 0002131, 0002133, and 0002139.

Department Goal for 2013 as: “Ensure the organization is PCI compliant by the end of Q2 2013”, suggesting that LifeLock was not compliant at the time.¹⁵⁸

Later, in May 2013, (b)(3);6(f),
(b)(4) PCI Gap Analysis Report concluded that LifeLock was not compliant in several key areas:¹⁵⁹



The Gap Analysis findings included the following:

- “LifeLock’s documented system security standards are not maintained or regularly updated, nor are they owned/provided by the Information Security department. The standards do not meet industry best practices or recommended hardening guidelines by system vendors.”
- “LifeLock is not performing security scans before major system or code changes are released into the CDE environment.”
- “There are Generic IDs utilized in LifeLock systems that are part of the CDE.”¹⁶⁰

¹⁵⁸ Att. 53, LifeLock, Security Department Goals 2013 (Jan. 30, 2013) (LIFELOCK-0010416-18) at LIFELOCK-0010416.

¹⁵⁹ Att. 44, PCI DSS Gap Analysis Report, (b)(3);6(f),(b)(4) (May 21, 2013) (LIFELOCK-0095891-959) at LIFELOCK-0095895.

¹⁶⁰ *Id.* at LIFELOCK-095896-87.

160. Even in March 2014, LifeLock’s internal risk assessment showed that it still lacked some of the most basic information security safeguards. LifeLock’s 2014 Enterprise Risk Assessment Summary Report states that “[t]here is a lack of daily security operational procedures” and that “[v]ulnerability scans are not conducted on corporate systems.”¹⁶¹

LifeLock’s ISP Deficiencies Enabled the Ransomware Attack in Late 2014

161. Predictably, LifeLock’s failure to meet minimum security standards led to the ransomware attack that occurred in late September 2014. The incident illustrates a number of the deficiencies in LifeLock’s ISP discussed above. LifeLock describes the attack as follows:¹⁶²

The attack began on September 23, 2014 at 12:37 p.m. when (b)(3)-6(f),(b)(4) (who is a LifeLock Resolution Specialist I, Member Services) browsed to a website that contained a malicious ad redirect. Within this same minute, the malware was downloaded and unpacked into memory in the process of execution. The attack was detected by LifeLock on November 4th at approximately 8:48 a.m.

162. The malware (Cryptowall) had access to all of the drives that (b)(3)-6(f),(b)(4) had access to, including the (b)(3) and (b)(3) drives containing members’ personal information, that typically included (b)(3)-6(f),(b)(4)

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

¹⁶¹ Att. 54, LifeLock, 2014 Enterprise Risk Assessment Summary Report, by Anne Marie Olson (Mar. 12, 2014) (LIFELOCK-0079743-44) at LIFELOCK-0079744.

¹⁶² Att. 36, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Federal Trade Commission, (Jan. 2, 2015) (LIFELOCK-0134224-40) at LIFELOCK-0134225.

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

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

The attacker encrypted

files and demanded a ransom to unencrypt the files. LifeLock only discovered the attack six weeks later and by happenstance when a LifeLock Resolution Specialist tried to open an encrypted file.¹⁶⁵

163. The attack exploited a vulnerability in the outdated Adobe Flash software that LifeLock used in its system.¹⁶⁶ At the time of the attack, LifeLock had not updated its Adobe Flash Player for over 6 months and was using version 12.0.0.4 which was more than 3 versions behind.¹⁶⁷ Adobe had released the following versions prior to the attack:

- a. Flash Player 15 released September 9, 2014¹⁶⁸
- b. Flash Player 14 released June 10, 2014¹⁶⁹
- c. Flash Player 13 released April 8, 2014¹⁷⁰

¹⁶³ *Id.* at LIFELOCK-0134233-34.

¹⁶⁴ *Id.* LIFELOCK-0134234-35

¹⁶⁵ *Id.* at LIFELOCK-0134225

¹⁶⁶ Att. 46, Letter from Andrew Berg, Counsel to LifeLock, Inc., to Greg Madden, Federal Trade Commission (Dec. 9, 2014) (LIFELOCK-0134215-16) at LIFELOCK-0134216.

¹⁶⁷ Att. 36 at LIFELOCK-0134229.

¹⁶⁸ Adobe Systems, *Release Notes – Flash Player 15 Air 15* (viewed on Jul. 14, 2015) <https://helpx.adobe.com/flash-player/release-note/fp_15_air_15_release_notes.html>.

¹⁶⁹ Adobe Systems, *Release Notes – Flash Player 14 Air 14* (viewed on Jul. 14, 2015) <https://helpx.adobe.com/flash-player/release-note/fp_14_air_14_release_notes.html>.

¹⁷⁰ Adobe Systems, *Release Notes – Flash Player 13 Air 13* (viewed on Jul. 14, 2015) <https://helpx.adobe.com/flash-player/release-note/fp_13_air_13_release_notes.html>.

164. At the request of LifeLock, (b)(3);6(f),
(b)(4) investigated the attack and determined that the attack would not have occurred if LifeLock had been using Adobe Flash version 13.0.0.26 or later.¹⁷¹ Adobe released version 13.0.0.26 on April 28, 2014 with a warning that the vulnerabilities addressed by the new version “could potentially allow an attacker to take control of the system.”¹⁷² The vulnerability was rated “critical” which meant that an attacker could potentially exploit the vulnerability without knowledge of the user.¹⁷³ Adobe gave the new version its highest priority rating of 1 which indicates that the vulnerability was currently being targeted or at a higher risk of being targeted than other vulnerabilities.¹⁷⁴ Accordingly, Adobe recommended that “administrators install the update as soon as possible. (for example, within 72 hours).”¹⁷⁵ On the day of the attack, almost 5 months after the release of this update, LifeLock still had the outdated version 12.0.0.4 running.

165. A major part of the reason that LifeLock missed so many critical updates to its Adobe Flash Player is that LifeLock again, like in 2012-2013, had technical problems with its patch deployment system. On October 9, 2014, LifeLock

¹⁷¹ Att. 55, *DLA Piper, LLC - Digital Forensic Investigation Report*, (b)(3);6(f),(b)(4) (Nov. 26, 2014) (LIFELOCK-0135499-510) at LIFELOCK-0135509. In the course of their investigation, (b)(3);6(f),
(b)(4) also discovered a number of other vulnerabilities on the compromised computer, noting “Java is out of date and is vulnerable to attack” and “[m]ultiple applications were out of date on the local endpoint.” *Id.*

¹⁷² Att. 56, Adobe Systems, *Adobe Security Bulletin* (released on Apr. 28, 2014) (FTC-0002088-93) at FTC-0002088.

¹⁷³ *Id.* at FTC-0002090, 0002092.

¹⁷⁴ *Id.* at FTC-0002089, 0002092

¹⁷⁵ *Id.* at FTC-0002092.

discovered Adobe’s System Center Updates Publisher “received an internal application error and refused to publish updates to the (b)(3):6(f), (b)(4) server.”¹⁷⁶ Over a month later, after failing to fix the technical problems with its patch deployment system, and after becoming aware of the ransomware attack exploiting this vulnerability, LifeLock manually updated Adobe Flash on November 11, 2014.¹⁷⁷

166. Compounding LifeLock’s failure to update its Adobe Flash was the fact that its vulnerability detection software, (b)(3):6(f),(b)(4) was misconfigured and could not detect the vulnerability caused by the outdated Adobe Flash. In order to scan servers for vulnerabilities, (b)(3):6(f),(b)(4) must have the right credentials for accessing the domain on which the servers reside. At the time of the attack, the (b)(3):6(f),(b)(4) servers with the Adobe Flash vulnerability resided on the (b)(3):6(f),(b)(4) domain. LifeLock, however, failed to give (b)(3):6(f),(b)(4) the credentials for the (b)(3):6(f),(b)(4) domain because it mistakenly thought the (b)(3):6(f),(b)(4) servers resided on the (b)(3):6(f),(b)(4) domain.¹⁷⁸

167. LifeLock’s (b)(3):6(f),(b)(4) should have detected this attack. The fact that it took LifeLock over a month to detect the attack, and that the detection occurred by happenstance when an employee attempted to open an encrypted file, indicates that LifeLock was either not monitoring its (b)(3):6(f),(b)(4) alerts, or as explained in

¹⁷⁶ Att. 36 at LIFELOCK-0134231.

¹⁷⁷ *Id.*

¹⁷⁸ *Id.* at LIFELOCK-0134232.

Paragraph 144, that (b)(3):6(f),(b)(4) was not properly configured to effectively protect LifeLock's network. This attack was a well-known, visible attack and should have been detected by (b)(3):6(f),(b)(4) soon after it had occurred.

168. LifeLock also did not appear to have the most current signatures for (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) 79 (b)(3):6(f),(b)(4) stops malware attacks by preventing the downloading or launching of code that matches the characteristics unique to each malware identified in its database. (b)(3):6(f),(b)(4) updated its malware signature database with the signature for Cryptowall, the malware that attacked LifeLock's network, on June 19, 2014, over three months prior to the attack.¹⁸⁰ If LifeLock had updated the malware signatures, (b)(3):6(f),(b)(4) would have stopped the attack.

Conclusion

169. Based on the evidence discussed above, LifeLock's ISP fell below minimum information security industry standards for at least the period from October 2012 through March 2014 for the following reasons:

- a. LifeLock did not have an effective vulnerability remediation process resulting in a failure to identify and fix vulnerabilities in a timely manner;

¹⁸⁰ Att. 57, (b)(3):6(f),(b)(4) (updated Mar. 3, 2015) (FTC-0002870-73).
¹⁸⁰ Att. 57, (b)(3):6(f),(b)(4) (updated Mar. 3, 2015) (FTC-0002870-73).

- b. LifeLock's patch management process was broken and incapable of applying necessary software patches and updates in a timely manner;
- c. LifeLock's configuration management process had multiple deficiencies, including lack of a consistent and formalized change management process and failure to remove vendor software default parameters and unneeded services; and
- d. LifeLock did not properly manage passwords, including passwords for users with administrative or manager credentials.

170. Because LifeLock fell below the minimum information security standard, LifeLock also did not meet the information security standard customary for financial institutions. ISPs of financial institutions typically exceed the minimum security standard by implementing additional security components and requiring shorter timeframes for applying patches and remediating vulnerabilities. For instance, a typical financial institution will remediate critical vulnerabilities within 15 days from discovery. If a full remediation would take a longer period of time, a mitigating measure would be put in place within the 15 day timeframe. Given the deficiencies described above, LifeLock clearly did not meet the higher standard for information security implemented by financial institutions.

171. LifeLock should not have received its PCI AOC in 2013. LifeLock failed to meet a number of PCI DSS requirements, including remediation of penetration test vulnerabilities, scanning of all VLANs, and patching of all critical patches

within 30 days. The serious delays in LifeLock's vulnerability remediation process also indicate that LifeLock did not continuously meet PCI DSS requirements from 2012 through 2014.

172. In my opinion, these failures were due in significant part to the following characteristics of LifeLock's ISP during that time period:

- *Lack of processes and formal security procedures.* Formal processes and procedures should drive security within an organization and ensure security is implemented and properly maintained. An information security program must implement processes identifying the tasks needing to be performed and the specific methods for accomplishing those tasks. Written procedures need to be developed **and followed** to ensure security is implemented in a consistent scalable manner. Based on the information I reviewed, LifeLock followed little to no formal processes in implementing their information security program. Many of LifeLock's security program elements were informal, ad-hoc, and manually driven processes. Formal security processes are automated, performed regularly, and schedule driven.
- *Third party assessments driving security.* Internal organizational assessments should drive an organization's information security implementation. External organizational assessments should provide validation that information security is being properly implemented. At LifeLock, third party assessments were used to determine security needs, as evidenced by the remediation efforts driven by the PCI Gap Analysis.

Third party assessments should not be the driver behind the security program because, *inter alia*, they are not performed frequently enough for remediating critical risks. Once a year assessments mean that the organization could be exposed for up to a year before a problem is identified.

- *Reactive vs proactive approach to information security.* With the threat vectors that exist today, organizations need to proactively identify and fix security problems. With the sensitive client information LifeLock receives, a proactive security approach is necessary to: identify problems, perform risk analysis, identify timeframes for reducing each risk, and use risk analysis to drive change across the organization. An organization of LifeLock's size and business should use full internal risk assessments as the primary driver for information security, with third party assessments, like PCI compliance, serving as a validation point.

I declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing
is true and correct.

Executed on: July 18, 2015



Dr. Eric B. Cole

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

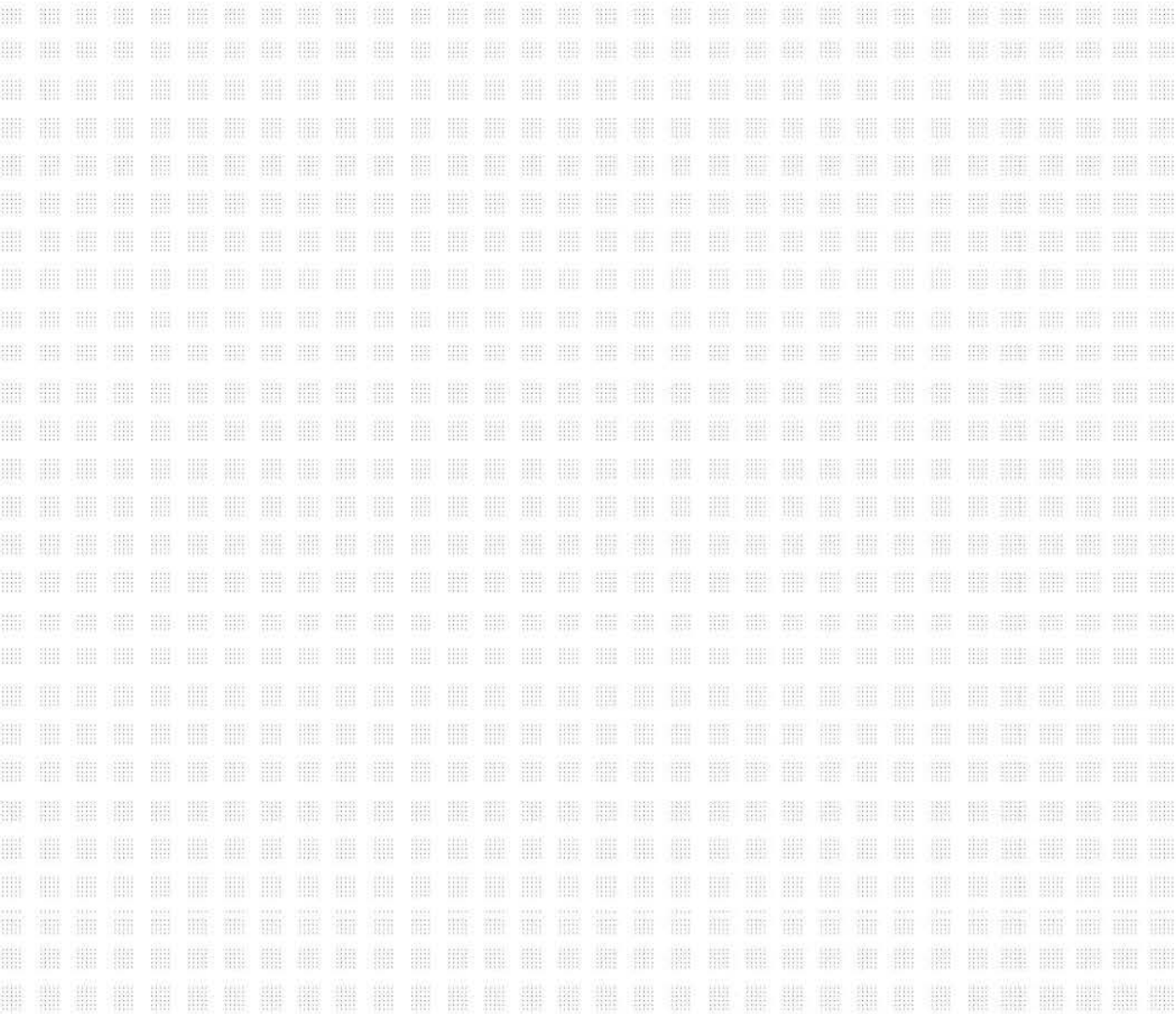
**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __22__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

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



Gwen Ceylon, CISSP CISM CISA
Contractor - Information Security/Compliance
480.457.2101 Office | (b)(6),(b)(7)(C) Cell
gwen.ceylon@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281
LifeLock® - Relentlessly Protecting Your Identity™

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __23__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

From: (b)(3):6(f),(b)(4)
Sent: Thursday, June 06, 2013 8:28 PM
To: Austin.Appel@lifelock.com
Subject: Updated (b)(3):6(f),(b) Request: 81561 (VRR **REDACTED** Security Updates (low))

Austin Appel,

Your support request has been **updated**. The details of your request are below.

The status of this request can be tracked here:

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

Request ID: 81561

Request Type: Service Request
Priority: Low

Category: Information Security
Sub-Category: Vulnerability Remediation Requests
Item:

Group Assigned: Information Security

Technician Assigned: Austin Appel

Subject: VRR (**REDACTED**) Security Updates (low)

Description:

Machine Name and/or IP:
REDACTED

Discovery Method & Date:
Internal PCI Scan on Oct 11, 2012

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6(f),(b)(4)

Description & Remediation Info:
MS10-077: Vulnerability in .NET Framework Could Allow Remote Code Execution (KB2160841)
MS11-028: Vulnerability in .NET Framework could allow remote code execution
MS11-039: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)
MS11-078: Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)

MS11-100: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)
MS12-016: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)
MS12-025: Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)
MS12-035: Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)
MS12-036: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)
MS12-038: Vulnerability in .NET Framework Could Allow Remote Code Execution (2706726)
MS12-045: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (2698365)
MS12-048: Vulnerability in Windows Shell Could Allow Remote Code Execution (2691442)
MS12-041: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)
MS12-047: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)
MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)
MS12-049: Vulnerability in TLS Could Allow Information Disclosure (2655992)
MS12-052: Cumulative Security Update for Internet Explorer (2722913)
MS12-054: Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)
MS12-055: Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)
MS12-056: Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution (2706045)

Apply the appropriate patches or remove the vulnerable packages if not needed

Thank you for contacting LifeLock Support.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __24__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

CONFIDENTIAL

From: (b)(3) 6(f), (b)(4)
Sent: Friday, June 07, 2013 1:21 PM
To: tony.valentine@lifelock.com
Subject: New items were added to 'From Hoyt'

(b)(3) 6(f), (b)(4) has added a new file, 'New QSA Punch List.docx'

File name: New QSA Punch List.docx
Path: All Files / Tony Valentine / 2013 PCI AUDIT / ADMIN, GENERAL / From (b)(3) 6(f), (b)(4)
Uploaded by: (b)(3) 6(f), (b)(4)
Upload date: 1:21 PM (GMT-07:00 MST) on Jun 7, 2013

[View File](#)

To access this file or add a comment, please visit:
(b)(3) 6(f), (b)(4)

Box Simple, Secure Sharing from Anywhere

You can change email preferences by visiting (b)(3) 6(f), (b)(4)

LIFELOCK-0022952

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __25__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __26__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 01, 2013 10:15 AM
To: (b)(3):6(f),(b)(4); Houcine Soudane; (b)(3):6(f),(b)(4); Mathew Stein; Prashanth Paladi; Andrew Ureta; Jim Casselbury; Jim Shoemaker; Jim Wrona; Patrick Sereno; (b)(3):6(f),(b)(4); Louis McNair; Tim Oliver; (b)(3):6(f),(b)(4); Justin Hyland; Nathan Shimek; (b)(3):6(f),(b)(4); Srinivas Gadiraju; (b)(3):6(f),(b)(4)
Cc: (b)(3):6(f),(b)(4); Nathan Shimek
Subject: Austin Appel; AnneMarie Olson; David Bridgman; Michael Peters; Rich Stebbins
VRR Process Changes

To all remediation teams:

In efforts to better align our VRR process with PCI requirements and our ever-changing environment, there have been some refinements to the VRR process which are addressed below.

- Frequency of scans
 - (b)(3):6(f),(b)(4)
- SLAs
 - Critical VRRs should be remediated within 30 days
 - High VRRs should be remediated within 60 days
 - Medium and Low VRRs should be remediated within 90 days.
 - If InfoSec (or any team) determines that a vulnerability has an immediate threat, we will work with the appropriate Infrastructure team to create an action plan to remediate as soon as possible.
- How vulnerabilities are classified
 - We will mainly be using the criticality rating as dictated by the Nexpose service rather than downgrading instantly due to known compensating controls and other factors.
 - What this means is that there will be more "highs" and "criticals".
 - You can request a downgrade of a rating. Your request must include a business justification.
- (b)(3):6(f),(b)(4)
 - All VRR tickets are now Category: Information Security; SubCategory: Vulnerability Remediation Requests
 - Due to changes within (b)(3):6(f),(b)(4) classifying the criticality of VRRs doesn't exactly match the tool. As such this is how we are handling tickets:
 - All VRRs have the true criticality listed in the subject name
 - For example: VRR **REDACTED** (b)(3):6(f),(b)(4) default installation/welcome page installed - **(high)**
 - The "Priority" Field is to be ignored (this is now auto-generated)
 - The Urgency Field is where the criticality is listed now
 - Critical VRRs will have an urgency of "High"
 - High VRRs will have an urgency of "Medium"

CONFIDENTIAL

- Both Medium and Low VRRs will have an urgency of "Low"
- VRR-specific groups have been eliminated – tickets will go in your regular queues

Please let Austin Appel or me know if you have any questions or concerns.

Thank you!

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __28__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Exhibit also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __29__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Exhibit also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT _30_ TO MEMORANDUM IN SUPPORT OF
ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

CONFIDENTIAL

From: Gwen Ceylon [/O=LIFELOCK/OU=EXCHANGE ADMINISTRATIVE GROUP
SENT =RECIPIENTS/CN=GWEN.CEYLON]
Sent: Friday, January 04, 2013 1:46 PM
To: Tony Valentine
Subject: Pen Tests Results Remediation Plan.xlsx
Attachments: Pen Tests Results Remediation Plan.xlsx

Tony,

I'm going to drive remediation for the findings from the Pen Tests also. Their attached with my additional comments on the findings. I'm tired of pussy footing around. Pen tests were in September – hello, it's January of the following year.

I'm putting a monster tracking spreadsheet together. I'll add the items from the risk assessment, the vulnerabilities scans, the pen tests, and the E&Y audit (if you want) – then I'm going to put my Doberman teeth in and get to cracking on remediation.

Let me have the E&Y spreadsheet – I like their format. Let's use that as a template for tracking everything.

Gwen

LIFELOCK-0038509

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __31__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

CONFIDENTIAL

From: (b)(3):6(f),(b)(4)
Sent: Wednesday, March 06, 2013 9:09 AM
To: Rich Stebbins; (b)(3):6(f),(b)(4); Renee Ramirez
Subject: PLEASE READ FOR APPROVAL OR FURTHER DISCUSSION: Vulnerability Remediation and Patch Management -- for PCI Readiness
Importance: High

Good Morning Everyone,

As part of PCI Readiness LifeLock must have a quarterly vulnerability scan and remediate vulnerabilities through system changes or by patching the systems.

For various reasons (ISI for example) patching for Windows and Linux systems have gotten behind, at least by 3 months. PCI requires that High, Medium and Low vulnerabilities be remediated in 30, 60, 90 days respectively. What this means is that LifeLock is behind in remediating most vulnerabilities (all high, most mediums and lows) and the remediation efforts need to be complete in this quarter (by end of March) so that we have a clean scan/remediation to provide to the (b)(3):6(f),(b)(4).

I have been working with Information Security (Austin) and with key personnel on (b)(3):6(f),(b)(4) to get back into a regular patching / vulnerability remediation cycle. The guys were challenged 2 weeks ago to review the new scans that Austin provided, patches that still need to be applied, and systems that need to be patched and how the systems could be grouped to patched.

(b)(3):6(f),(b)(4) raised issues that they encounter (not just during this two weeks but issues that have come up in the past) that pushes back their patching efforts. They also provided me with two solutions that I am coming to all of you with for review, comments/changes, and hopefully approval.

PLEASE REVIEW AND COMMENT/APPROVE. If you approve, I believe that (b)(3):6(f) and Renee will need to work out the logistics for their teams and communications.

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

Again, I know that both of these requests are a bit out of the norm and can be challenging if not properly managed, especially with communications to appropriate teams. That is why I suggest (b)(3):6(f) and Renee work together to talk about challenges, impacts, and coordination.

LIFELOCK-0019638

CONFIDENTIAL

You all are very busy but if you wish to have a deeper discussion about this topic please let me know and I will schedule all of you (and others if you wish). We have 3 weeks left to remediate in the first quarter so I would like to meet today, tomorrow or latest on Friday if possible.

Thank you everyone!

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

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Federal Trade Commission,

Plaintiff,

v.

LifeLock, Inc., *et al*,

Defendants.

No. CV-10-00530-PHX-MHM

**FEDERAL TRADE COMMISSION'S
MOTION FOR CONTEMPT AGAINST
LIFELOCK, INC.**

LODGED UNDER SEAL

**FTC PROPOSED EXHIBIT __32__ TO MEMORANDUM IN SUPPORT
OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

**DECLARATION OF ELIZABETH ANNE MILES
PURSUANT TO 28 U.S.C. § 1746**

I, Elizabeth Anne Miles, hereby declare as follows:

1. I am a citizen of the United States and am over eighteen years of age. Unless stated otherwise, I have personal knowledge of the facts contained in this Declaration. If called as a witness, I could and would testify to the facts stated herein.

2. I am a data analyst with the Federal Trade Commission (“FTC”), in the Bureau of Consumer Protection. I have been an employee of the FTC since December 2005. Among other things, my job involves the analysis of electronic information stored on computer systems and related data storage devices/media.

3. My formal education includes a bachelor’s degree in Economics and Spanish from the University of Kentucky and a graduate certificate in Geographic Information Sciences from George Mason University.

Alert Gap Analysis

4. I was asked by FTC counsel to analyze data provided by LifeLock on gaps in their alerting services and provide basic summary statistics on these data.

5. The data was provided to the FTC as Annex 3 and Annex 18 to LifeLock’s July 2, 2014, response to the FTC (“July 2 Letter”). Both sets of data appear to have originated as spreadsheet tables, but were provided to the FTC as part of a PDF. See Exhibit A (LifeLock’s July 2, 2014, Annex 3) and Exhibit B (LifeLock’s July 2, 2014, Annex 18). According to LifeLock’s July 2 Letter, Annex 3 documents all periods between October 2012 and March 2014 when there was an hour of the day where no LifeLock alerts were sent out (e.g., if there were no alerts sent out between 1:00am and 1:59am) and contains gaps in both LifeLock’s IDA alerts and EWS alerts. Annex 18 to the July 2 Letter lists 42 weekends in which no EWS alerts were

processed. Each gap was more than 60 hours in potential duration and typically spanned from Friday evening to Monday morning. Each EWS gap was also listed in Annex 3.

6. In the original presentation of Annex 3 from the July 2 Letter, the tables contained columns indicating a label, the start date and time of the gap, the end date and time of the gap, LifeLock's calculation of the potential duration of the gap, the number of alerts processed during the time frame, the number of members impacted, and a note field. The tables were structured with rows alternating between an "Alert Gap", with most of the information listed above, then "Alert processed after gap" indicating a start date and time, the number of alerts processed, and number of members impacted.

7. FTC staff converted Annex 3 from the July 2 Letter from a PDF to a Microsoft Excel spreadsheet. I spot-checked several rows of the table to ensure they had been converted correctly.

8. I conducted my analysis of the gap data using Microsoft Excel. I first categorized the gaps by the potential duration of the gap and by the presence or absence of the word "planned" in the notes field (i.e. "Planned Maintenance"). I then conducted basic cross-tabulations for these categories.

9. Based on the data contained in LifeLock's Annex 3, during the period covered, there were 1,258 gaps of at least an hour in LifeLock's data. Of these 1,258 gaps, 679 gaps were 1 hour in duration and 182 gaps were 2 hours.

10. The data shows LifeLock had 287 gaps of 5 hours or longer during the relevant period, and, as stated above, 42 weekend gaps of more than 60 hours in which EWS alerts were not processed.

11. Exhibit C to this declaration shows the number of alert gaps, whether they were planned, unplanned, and in total for gaps of any duration, gaps 5-9 hours, gaps 10-59 hours and gaps 60 or more hours in Annex 3.

12. Of the 1,258 alert gaps, 28.0% at least partially overlapped the hours of 8am to 6pm.

VRR Analysis

13. FTC counsel also asked me to analyze data provided by LifeLock on the status of Vulnerability Remediation Request (VRR) tickets that were opened between April 2012 and May 2015.

14. The data I reviewed were contained in two Excel spreadsheet files, “gmLIFELOCK-0135783.xlsx” and “hpLifelock-0135784-86.xlsx”,¹ and two CSV files, “LIFELOCK-0138077.csv” and “LIFELOCK-0138078.csv”. The Excel file “hpLifelock-0135784-86.xlsx” contained three worksheets, labelled with Bates numbers “Lifelock-0135784”, “Lifelock-0135785”, and “Lifelock-0135786”, while the other Excel file had only one worksheet. All four files contained columns for “Request ID”, “Created Time”, “Subcategory”, “Subject”, “Description”,² “Requester”, “Technician”, “Request Status”, “Resolution”, “Completed Time”, “Note”, “Date of Note”, and “Note Added By”. The rows were grouped by Request ID, with the ID initially appearing alone on a row, then followed by one or more rows with information on that request ID. Where more than one row was present, all columns were duplicated except for those relating to the Note.

¹ I compared “gmLIFELOCK-0135783.xlsx” with “Lifelock-0135783.csv” using Microsoft Excel and found that the data in the two files were identical. Using the same method, I also confirmed that “hpLifelock-0135784-86.xlsx” contained the same data as “Lifelock-0135784.csv”, “Lifelock-0135785.csv”, and “Lifelock-0135786.csv”. The four CSV files were Attachment 13 to the Expert Report of Dr. Eric B. Cole.

² In some of the files, this was rendered as “Request Description”, but appeared in the same position and had similar content.

15. I appended the VRR ticket data from the separate files and worksheets into one Excel file. I made manual corrections to two records. In “gmLIFELOCK-0135783.xlsx”, the text for the “Description” field in row 769 was so long that it had exceeded the maximum length for an Excel field and broke onto another line, with the last several sentences appearing in the “Request ID” field in row 771, and the remaining fields following “Description” appearing in the columns next to “Request ID”. Because the excess “Description” text did not appear relevant to my analysis, I deleted this text and transferred the remaining fields to the appropriate columns in row 769. I performed the same type of correction to row 1,554 of “LIFELOCK-0138078.csv”.

16. I removed 1,741 duplicated records from the appended Excel file. By duplicate record, I mean the information in every column from “Request ID” to “Note Added By” was identical to the information in another record.

17. I dropped 2,719 records that did not have a “Created Time”, including the header row for each ticket.

18. I used Excel’s Find and Replace function to change each instance of “N/A” to blank.

19. I imported the appended VRR log data from the Excel file I created into Stata, a common statistical software package. Before beginning my analysis, I took the following steps to clean the data in Stata:

- a. I dropped 116 tickets for which the “Subcategory” field did not state “Vulnerability Remediation Request” or for which “Description” field did not have the text “Discovery Method & Date” which is found in that field for a “Vulnerability Remediation Request” ticket.

- b. I dropped tickets with the words “duplicate”, “ignore”, or “test” in the “Subject” field, and I dropped tickets with the word “duplicate” in the “Resolution” field. Thirty-eight tickets were dropped.
- c. I flagged a single instance of the same “Request ID”, so that each unique ticket could be counted once.
- d. I used a text matching function to extract the criticality of each ticket from the “Subject” field. Most tickets contained the word “critical”, “high”, “medium”, or “low” in parentheses at the end of the “Subject” field, and I extracted whatever was in the parentheses into a new field.
- e. Using a text matching function, I extracted the vulnerability discovery date from the “Description” field into a new field. In most tickets, a discovery date was listed near the beginning of the “Description” field in a form similar to:

Machine Name and/or IP: (b)(3),6(f),(b)(4) Discovery Method &
Date: Internal PCI scan on April 4th, 2013 Vulnerability Details...”

I created a matching logic using Stata’s text matching functions to extract any date contained in this type of text. Dates that were not readily matched by the computer but were easy to identify by the human eye were captured manually.

- f. Using a similar process to the one described above, I used Stata’s text matching functions to extract a date, if any existed, from the “Resolution” into a new field. A common form of this field with the date might be “Resolution verified by Internal PCI Scan on 10/31/13”.

20. Once the data was cleaned, I used to Stata to analyze the data as described in the following paragraphs.

21. I determined the oldest and newest “Created Time”, “Date of Note”, and “Completed Time” time in the data. A table of these dates is attached as Exhibit D to this declaration.

22. I counted the number of tickets by criticality and “Request Status”. Exhibit E to this declaration shows these counts.

23. For each ticket, I calculated several timeframes: the number of days from the date of discovery of the vulnerability as determined in Paragraph 19(e) to the date in “Created Time”, to the date in “Date of Note”, to the date of resolution as determined in Paragraph 19(f), and to the date in “Completed Time”; and the number of days from the date in “Created Time” to the date of resolution and the date in “Completed Time”. I used June 1, 2015 as the date of completion for tickets where “Request Status” was “Open”. For tickets that had a discovery date more than a year before the ticket “Created Time”, I assumed the discovery was incorrectly listed as a year earlier than its actual occurrence—all instances had a January or February discovery date. By calculating these timeframes for each ticket, I was able to generate the data analysis in Exhibits F, G, and H.

24. In Exhibit F, I calculated averages for each of these timeframes for each criticality level (critical, high, medium, and low). I also calculated averages for each of these timeframes for each quarter from second quarter of 2012 to second quarter of 2015.

25. In Exhibit G, I calculated the number of tickets with timeframes between vulnerability discovery to “Date of Note” greater than 30 days, 60 days, and 90 days. I performed this analysis separately for all tickets, for tickets by criticality level, and for all tickets by quarter from second quarter of 2012 to second quarter of 2015. I noted in the column labeled

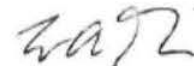
“Indeterminable” the number of tickets for which I could not perform this analysis because no date was included in either the “Description” field or the “Date of Note” field.

26. Similarly, in Exhibit H, I calculated the number of tickets with timeframes between vulnerability discovery to “Resolution” greater than 30 days, 60 days, and 90 days. I performed this analysis separately for all tickets, for tickets by criticality level, and for all tickets by quarter from second quarter of 2012 to second quarter of 2015. I noted in the column labeled “Indeterminable” the number of tickets for which I could not perform this analysis because no date was included in either the “Description” field or the “Resolution” field.

27. In Exhibit I, I calculated the number of “critical” or “high” criticality level tickets with the date in “Created Time” during September 1, 2012, through February 21, 2013, and separately for tickets with the date in “Created Time” during March 13, 2013, through June 25, 2013.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 15th day of July 2015.



Elizabeth Anne Miles

EXHIBIT A

Label	Start Date	Start Time	End Date	End Time	Potential Duration (in hrs)	# of Alerts Processed	# of Members Impacted	Notes
Alert Gap	10/6/2012	10:00 PM	10/6/2012	10:00 PM	1	0		(b)(3);6(f),(b)(4)
Alert processed after gap	10/6/2012	11:30 PM				2	2	
Alert Gap	10/16/2012	4:00 PM	10/16/2012	4:00 PM	1	0		
Alert processed after gap	10/16/2012	5:00 PM				319	318	
Alert Gap	10/16/2012	11:00 PM	10/17/2012	4:00 AM	6	0		
Alert processed after gap	10/17/2012	5:00 AM				393	391	
Alert Gap	10/18/2012	11:00 PM	10/19/2012	12:00 AM	2	0		
Alert processed after gap	10/19/2012	1:15 AM				64	64	
Alert Gap	10/24/2012	12:00 AM	10/24/2012	12:00 AM	1	0		
Alert processed after gap	10/24/2012	1:15 AM				94	94	
Alert Gap	10/26/2012	12:00 AM	10/26/2012	12:00 AM	1	0		
Alert processed after gap	10/26/2012	1:45 AM				47	47	
Alert Gap	11/8/2012	11:00 PM	11/9/2012	1:00 AM	3	0		
Alert processed after gap	11/9/2012	2:30 AM				106	104	
Alert Gap	11/11/2012	1:00 AM	11/11/2012	2:00 AM	2	0		
Alert processed after gap	11/11/2012	3:00 AM				63	63	
Alert Gap	11/14/2012	12:00 AM	11/14/2012	3:00 AM	4	0		
Alert processed after gap	11/14/2012	4:45 AM				101	99	
Alert Gap	11/15/2012	11:00 PM	11/16/2012	4:00 AM	5	0		
Alert processed after gap	11/16/2012	5:00 AM				131	129	
Alert Gap	11/20/2012	9:00 PM	11/21/2012	11:00 AM	15	0		
Alert processed after gap	11/21/2012	12:00 PM				573	573	
Alert Gap	11/29/2012	11:00 PM	11/30/2012	2:00 AM	4	0		
Alert processed after gap	11/30/2012	3:00 AM				164	164	
Alert Gap	12/4/2012	10:00 PM	12/5/2012	3:00 AM	6	0		
Alert processed after gap	12/5/2012	4:00 AM				187	184	

Alert Gap	12/5/2012	5:00 AM	12/5/2012	11:00 AM	7		
Alert processed after gap	12/5/2012	12:45 PM				618	615
Alert Gap	12/5/2012	10:00 PM	12/6/2012	3:00 AM	6		
Alert processed after gap	12/6/2012	4:00 AM				90	90
Alert Gap	12/6/2012	10:00 PM	12/7/2012	3:00 AM	6		
Alert processed after gap	12/7/2012	4:00 AM				365	363
Alert Gap	12/7/2012	10:00 PM	12/8/2012	3:00 AM	6		
Alert processed after gap	12/8/2012	4:00 AM				174	174
Alert Gap	12/8/2012	10:00 PM	12/9/2012	3:00 AM	6		
Alert processed after gap	12/9/2012	4:00 AM				93	93
Alert Gap	12/9/2012	10:00 PM	12/10/2012	3:00 AM	6		
Alert processed after gap	12/10/2012	4:00 AM				281	278
Alert Gap	12/10/2012	10:00 PM	12/11/2012	3:00 AM	6		
Alert processed after gap	12/11/2012	4:00 AM				212	211
Alert Gap	12/11/2012	10:00 PM	12/12/2012	2:00 AM	5		
Alert processed after gap	12/12/2012	3:15 AM				83	81
Alert Gap	12/13/2012	11:00 PM	12/14/2012	12:00 AM	2		
Alert processed after gap	12/14/2012	1:30 AM				101	101
Alert Gap	12/14/2012	11:00 PM	12/15/2012	12:00 AM	2		
Alert processed after gap	12/15/2012	1:30 AM				82	82
Alert Gap	12/15/2012	11:00 PM	12/15/2012	11:00 PM	1		
Alert processed after gap	12/16/2012	12:30 AM				27	27
Alert Gap	1/8/2013	11:00 PM	1/9/2013	3:00 AM	5		
Alert processed after gap	1/9/2013	4:00 AM				108	104
Alert Gap	1/10/2013	11:00 PM	1/11/2013	3:00 AM	5		
Alert processed after gap	1/11/2013	4:00 AM				141	139
Alert Gap	1/15/2013	5:00 AM	1/15/2013	11:00 AM	7		
Alert processed after gap	1/15/2013	12:00 PM				127	127
Alert Gap	1/17/2013	11:00 PM	1/18/2013	2:00 AM	4		

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

Alert processed after gap	1/18/2013	3:00 AM				110	109
Alert Gap	1/18/2013	11:00 PM	1/18/2013	11:00 PM	1		
Alert processed after gap	1/19/2013	12:30 AM				17	17
Alert Gap	1/20/2013	1:00 AM	1/20/2013	4:00 AM	4		
Alert processed after gap	1/20/2013	5:00 AM				163	163
Alert Gap	1/20/2013	11:00 PM	1/21/2013	4:00 AM	6		
Alert processed after gap	1/21/2013	5:00 AM				199	197
Alert Gap	1/21/2013	11:00 PM	1/22/2013	4:00 AM	6		
Alert processed after gap	1/22/2013	5:00 AM				332	329
Alert Gap	1/22/2013	11:00 PM	1/23/2013	2:00 AM	4		
Alert processed after gap	1/23/2013	3:00 AM				93	93
Alert Gap	1/24/2013	10:00 PM	1/25/2013	3:00 AM	6		
Alert processed after gap	1/25/2013	4:00 AM				125	125
Alert Gap	1/28/2013	10:00 PM	1/29/2013	5:00 AM	8		
Alert processed after gap	1/29/2013	6:30 AM				211	211
Alert Gap	1/31/2013	11:00 PM	2/1/2013	2:00 AM	4		
Alert processed after gap	2/1/2013	3:00 AM				115	115
Alert Gap	2/1/2013	11:00 PM	2/2/2013	2:00 AM	4		
Alert processed after gap	2/2/2013	3:00 AM				117	117
Alert Gap	2/2/2013	11:00 PM	2/3/2013	2:00 AM	4		
Alert processed after gap	2/3/2013	3:00 AM				81	81
Alert Gap	2/3/2013	11:00 PM	2/4/2013	2:00 AM	4		
Alert processed after gap	2/4/2013	3:00 AM				166	165
Alert Gap	2/9/2013	7:00 PM	2/9/2013	8:00 PM	2		
Alert processed after gap	2/9/2013	9:45 PM				128	128
Alert Gap	2/13/2013	12:00 AM	2/13/2013	3:00 AM	4		
Alert processed after gap	2/13/2013	4:15 AM				163	163
Alert Gap	2/14/2013	11:00 PM	2/15/2013	2:00 AM	4		
Alert processed after gap	2/15/2013	3:00 AM				98	96

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

Alert Gap	2/21/2013	11:00 PM	2/22/2013	2:00 AM	4		
Alert processed after gap	2/22/2013	3:00 AM				112	111
Alert Gap	2/26/2013	11:00 PM	2/27/2013	10:00 AM	12		
Alert processed after gap	2/27/2013	11:00 AM				322	318
Alert Gap	3/7/2013	10:00 PM	3/8/2013	3:00 AM	5		
Alert processed after gap	3/8/2013	4:00 AM				140	139
Alert Gap	3/12/2013	5:00 AM	3/12/2013	6:00 PM	2		
Alert processed after gap	3/12/2013	7:45 PM				328	326
Alert Gap	3/15/2013	12:00 AM	3/15/2013	1:00 AM	2		
Alert processed after gap	3/15/2013	2:30 AM				104	104
Alert Gap	3/19/2013	11:00 PM	3/20/2013	2:00 AM	4		
Alert processed after gap	3/20/2013	3:00 AM				102	102
Alert Gap	3/20/2013	11:00 PM	3/21/2013	2:00 AM	4		
Alert processed after gap	3/21/2013	3:00 AM				295	295
Alert Gap	3/21/2013	11:00 PM	3/22/2013	4:00 AM	6		
Alert processed after gap	3/22/2013	5:30 AM				201	200
Alert Gap	3/23/2013	8:00 PM	3/25/2013	9:00 AM	38		
Alert processed after gap	3/25/2013	10:00 AM				515	513
Alert Gap	3/26/2013	1:00 AM	3/26/2013	1:00 AM	1		
Alert processed after gap	3/26/2013	2:15 AM				36	36
Alert Gap	3/27/2013	12:00 PM	3/27/2013	1:00 PM	2		
Alert processed after gap	3/27/2013	2:00 PM				562	558
Alert Gap	3/28/2013	11:00 PM	3/29/2013	6:00 AM	8		
Alert processed after gap	3/29/2013	7:45 AM				101	100
Alert Gap	3/29/2013	11:00 PM	3/30/2013	2:00 AM	4		
Alert processed after gap	3/30/2013	3:00 AM				121	119
Alert Gap	3/30/2013	11:00 PM	3/31/2013	2:00 AM	4		
Alert processed after gap	3/31/2013	3:00 AM				207	207
Alert Gap	3/31/2013	11:00 PM	4/1/2013	2:00 AM	4		

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

Alert processed after gap	4/1/2013	3:00 AM				32	32
Alert Gap	4/1/2013	6:00 AM	4/1/2013	6:00 AM	1		
Alert processed after gap	4/1/2013	7:30 AM				66	66
Alert Gap	4/3/2013	11:00 PM	4/4/2013	2:00 AM	4		
Alert processed after gap	4/4/2013	3:00 AM				158	158
Alert Gap	4/4/2013	11:00 PM	4/5/2013	2:00 AM	4		
Alert processed after gap	4/5/2013	3:00 AM				99	98
Alert Gap	4/11/2013	10:00 PM	4/12/2013	4:00 AM	7		
Alert processed after gap	4/12/2013	5:00 AM				285	284
Alert Gap	4/16/2013	8:00 PM	4/16/2013	8:00 PM	1		
Alert processed after gap	4/16/2013	9:00 PM				49	49
Alert Gap	4/17/2013	12:00 AM	4/17/2013	7:00 AM	8		
Alert processed after gap	4/17/2013	8:15 AM				164	162
Alert Gap	4/17/2013	9:00 AM	4/17/2013	9:00 AM	1		
Alert processed after gap	4/17/2013	10:00 AM				74	73
Alert Gap	4/17/2013	11:00 AM	4/17/2013	11:00 AM	1		
Alert processed after gap	4/17/2013	12:15 PM				351	349
Alert Gap	4/18/2013	7:00 PM	4/18/2013	8:00 PM	2		
Alert processed after gap	4/18/2013	9:30 PM				121	119
Alert Gap	4/19/2013	1:00 AM	4/19/2013	1:00 AM	1		
Alert processed after gap	4/19/2013	2:00 AM				95	95
Alert Gap	4/21/2013	1:00 AM	4/21/2013	1:00 AM	1		
Alert processed after gap	4/21/2013	2:00 AM				7	7
Alert Gap	4/21/2013	3:00 AM	4/21/2013	8:00 AM	6		
Alert processed after gap	4/21/2013	9:45 AM				510	503
Alert Gap	4/22/2013	1:00 AM	4/22/2013	7:00 AM	7		
Alert processed after gap	4/22/2013	8:30 AM				341	339
Alert Gap	4/22/2013	9:00 AM	4/22/2013	9:00 AM	1		
Alert processed after gap	4/22/2013	10:00 AM				164	164

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

Alert Gap	4/22/2013	12:00 PM	4/22/2013	12:00 PM	1			(b)(3);6(f),(b)(4)
Alert processed after gap	4/22/2013	1:00 PM				328	325	
Alert Gap	4/25/2013	11:00 PM	4/26/2013	3:00 AM	5			
Alert processed after gap	4/26/2013	4:00 AM				120	120	
Alert Gap	5/1/2013	10:00 AM	5/1/2013	12:00 PM	3			
Alert processed after gap	5/1/2013	1:00 PM				228	227	
Alert Gap	5/4/2013	5:00 AM	5/4/2013	7:00 AM	3			
Alert processed after gap	5/4/2013	8:00 AM				88	88	
Alert Gap	5/7/2013	10:00 PM	5/8/2013	3:00 AM	6			
Alert processed after gap	5/8/2013	4:00 AM				127	125	
Alert Gap	5/11/2013	5:00 AM	5/11/2013	5:00 AM	1			
Alert processed after gap	5/11/2013	6:15 AM				50	50	
Alert Gap	5/11/2013	7:00 AM	5/11/2013	7:00 AM	1			
Alert processed after gap	5/11/2013	8:45 AM				301	300	
Alert Gap	5/13/2013	10:00 AM	5/13/2013	10:00 AM	1			
Alert processed after gap	5/13/2013	11:15 AM				164	164	
Alert Gap	5/13/2014	1:00 PM	5/13/2014	2:00 PM	2			
Alert processed after gap	5/13/2014	3:15 PM				483	478	
Alert Gap	5/14/2013	10:00 PM	5/15/2013	6:00 AM	9			
Alert processed after gap	5/15/2013	7:30 AM				108	108	
Alert Gap	5/16/2013	7:00 PM	5/16/2013	7:00 PM	1			
Alert processed after gap	5/16/2013	8:00 PM				45	45	
Alert Gap	5/20/2013	11:00 AM	5/20/2013	11:00 AM	1			
Alert processed after gap	5/20/2013	12:30 PM				249	247	
Alert Gap	5/21/2013	11:00 PM	5/22/2013	3:00 AM	5			
Alert processed after gap	5/22/2013	4:00 AM				229	228	
Alert Gap	5/23/2013	11:00 PM	5/24/2013	3:00 AM	5			
Alert processed after gap	5/24/2013	4:00 AM				134	134	
Alert Gap	6/5/2013	9:00 PM	6/6/2013	7:00 AM	11			

Alert processed after gap	6/6/2013	8:00 AM			1	1
Alert Gap	6/8/2013	11:00 AM	6/8/2013	12:00 PM	2	
Alert processed after gap	6/8/2013	1:15 PM			373	372
Alert Gap	6/10/2013	2:00 AM	6/10/2013	2:00 AM	1	
Alert processed after gap	6/10/2013	3:00 AM			1	1
Alert Gap	6/13/2013	9:00 PM	6/14/2013	7:00 AM	11	
Alert processed after gap	6/14/2013	8:00 AM			36	36
Alert Gap	6/18/2013	11:00 PM	6/19/2013	3:00 AM	5	
Alert processed after gap	6/19/2013	4:00 AM			139	139
Alert Gap	6/19/2013	11:00 PM	6/20/2013	3:00 AM	5	
Alert processed after gap	6/20/2013	4:00 AM			218	217
Alert Gap	6/20/2013	11:00 PM	6/21/2013	3:00 AM	5	
Alert processed after gap	6/21/2013	4:00 AM			88	88
Alert Gap	6/25/2013	6:00 PM	6/26/2013	4:00 AM	11	
Alert processed after gap	6/26/2013	5:30 AM			204	203
Alert Gap	6/27/2013	11:00 PM	6/28/2013	10:00 AM	12	
Alert processed after gap	6/28/2013	11:45 AM			124	123
Alert Gap	6/28/2013	11:00 PM	6/29/2013	3:00 AM	5	
Alert processed after gap	6/29/2013	4:00 AM			97	97
Alert Gap	6/29/2013	11:00 PM	6/30/2013	3:00 AM	5	
Alert processed after gap	6/30/2013	4:00 AM			66	66
Alert Gap	6/30/2013	11:00 PM	7/1/2013	3:00 AM	5	
Alert processed after gap	7/1/2013	4:00 AM			129	129
Alert Gap	7/4/2013	10:00 AM	7/4/2013	10:00 AM	1	
Alert processed after gap	7/4/2013	11:00 AM			257	257
Alert Gap	7/8/2013	9:00 PM	7/8/2013	9:00 PM	1	
Alert processed after gap	7/8/2013	10:00 PM			124	124
Alert Gap	7/9/2013	7:00 PM	7/10/2013	4:00 AM	10	
Alert processed after gap	7/10/2013	5:15 AM			239	233

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

Alert Gap	7/13/2013	10:00 PM	7/13/2013	10:00 PM	1			(b)(3);6(f),(b)(4)
Alert processed after gap	7/13/2013	11:00 PM				18	18	
Alert Gap	7/16/2013	11:00 PM	7/17/2013	3:00 AM	5			
Alert processed after gap	7/17/2013	4:00 AM				145	144	
Alert Gap	7/20/2013	9:00 PM	7/21/2013	6:00 AM	10			
Alert processed after gap	7/21/2013	7:00 AM				228	226	
Alert Gap	7/25/2013	3:00 PM	7/26/2013	4:00 AM	14			
Alert processed after gap	7/26/2013	5:30 AM				374	372	
Alert Gap	7/26/2013	7:00 AM	7/26/2013	7:00 AM	1			
Alert processed after gap	7/26/2013	8:00 AM				122	121	
Alert Gap	7/27/2013	11:00 PM	7/27/2013	11:00 PM	1			
Alert processed after gap	7/28/2013	12:30 AM				67	67	
Alert Gap	7/29/2013	8:00 PM	7/30/2013	2:00 AM	7			
Alert processed after gap	7/30/2013	3:45 AM				269	265	
Alert Gap	8/4/2013	9:00 PM	8/5/2013	4:00 AM	8			
Alert processed after gap	8/5/2013	5:30 AM				256	255	
Alert Gap	8/17/2013	11:00 PM	8/18/2013	12:00 AM	2			
Alert processed after gap	8/18/2013	1:00 AM				3	3	
Alert Gap	8/29/2013	7:00 PM	8/29/2013	7:00 PM	1			
Alert processed after gap	8/29/2013	8:00 PM				42	41	
Alert Gap	9/3/2013	11:00 PM	9/3/2013	11:00 PM	1			
Alert processed after gap	9/4/2013	12:30 AM				78	76	
Alert Gap	9/5/2013	11:00 PM	9/6/2013	3:00 AM	5			
Alert processed after gap	9/6/2013	4:00 AM				155	154	
Alert Gap	9/10/2013	7:00 PM	9/11/2013	4:00 AM	10			
Alert processed after gap	9/11/2013	5:30 AM				159	156	
Alert Gap	9/12/2013	8:00 PM	9/13/2013	8:00 AM	13			
Alert processed after gap	9/13/2013	9:15 AM				440	439	
Alert Gap	9/24/2013	8:00 PM	9/25/2013	7:00 AM	12			

Alert processed after gap	9/25/2013	8:00 AM				546	537
Alert Gap	9/26/2013	8:00 PM	9/27/2013	4:00 AM	9		
Alert processed after gap	9/27/2013	5:15 AM				352	351
Alert Gap	10/1/2013	11:00 PM	10/2/2013	3:00 AM	5		
Alert processed after gap	10/2/2013	4:00 AM				255	253
Alert Gap	10/2/2013	11:00 PM	10/3/2013	3:00 AM	5		
Alert processed after gap	10/3/2013	4:00 AM				149	147
Alert Gap	10/3/2013	11:00 PM	10/4/2013	3:00 AM	5		
Alert processed after gap	10/4/2013	4:00 AM				142	140
Alert Gap	10/4/2013	11:00 PM	10/5/2013	3:00 AM	5		
Alert processed after gap	10/5/2013	4:00 AM				132	131
Alert Gap	10/17/2013	10:00 PM	10/18/2013	3:00 AM	6		
Alert processed after gap	10/18/2013	4:00 AM				488	487
Alert Gap	10/24/2013	10:00 PM	10/24/2013	11:00 PM	2		
Alert processed after gap	10/25/2013	12:15 AM				1	1
Alert Gap	10/28/2013	11:00 PM	10/29/2013	9:00 AM	11		
Alert processed after gap	10/29/2013	10:30 AM				741	738
Alert Gap	10/29/2013	10:00 PM	10/30/2013	3:00 AM	6		
Alert processed after gap	10/30/2013	4:00 AM				531	527
Alert Gap	11/7/2013	7:00 PM	11/8/2013	4:00 AM	10		
Alert processed after gap	11/8/2013	5:00 AM				774	770
Alert Gap	11/8/2013	7:00 PM	11/9/2013	6:00 AM	12		
Alert processed after gap	11/9/2013	7:30 AM				659	656
Alert Gap	11/13/2013	9:00 PM	11/14/2013	3:00 AM	7		
Alert processed after gap	11/14/2013	4:00 AM				247	243
Alert Gap	11/19/2013	7:00 PM	11/20/2013	6:00 AM	12		
Alert processed after gap	11/20/2013	7:45 AM				1	1
Alert Gap	11/20/2013	12:00 PM	11/20/2013	12:00 PM	1		
Alert processed after gap	11/20/2013	1:15 PM				331	330

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

Alert Gap	11/20/2013	2:00 PM	11/20/2013	3:00 PM	2			(b)(3);6(f),(b)(4)
Alert processed after gap	11/20/2013	4:30 PM				246	245	
Alert Gap	11/21/2013	10:00 AM	11/21/2013	10:00 AM	1			
Alert processed after gap	11/21/2013	11:30 AM				316	316	
Alert Gap	11/26/2013	9:00 PM	11/27/2013	4:00 AM	8			
Alert processed after gap	11/27/2013	5:15 AM				428	423	
Alert Gap	12/5/2013	10:00 PM	12/6/2013	3:00 AM	6			
Alert processed after gap	12/6/2013	4:00 AM				545	540	
Alert Gap	12/6/2013	10:00 PM	12/7/2013	3:00 AM	6			
Alert processed after gap	12/7/2013	4:00 AM				530	528	
Alert Gap	12/7/2013	10:00 PM	12/8/2013	3:00 AM	6			
Alert processed after gap	12/8/2013	4:00 AM				362	360	
Alert Gap	12/8/2013	10:00 PM	12/8/2013	11:00 PM	2			
Alert processed after gap	12/9/2013	12:30 AM				117	115	
Alert Gap	12/10/2013	10:00 PM	12/11/2013	3:00 AM	6			
Alert processed after gap	12/11/2013	4:00 AM				823	817	
Alert Gap	12/11/2013	10:00 PM	12/12/2013	3:00 AM	6			
Alert processed after gap	12/12/2013	4:00 AM				273	268	
Alert Gap	12/12/2013	2:00 PM	12/12/2013	2:00 PM	1			
Alert processed after gap	12/12/2013	3:45 PM				632	626	
Alert Gap	12/12/2013	10:00 PM	12/13/2013	3:00 AM	6			
Alert processed after gap	12/13/2013	4:00 AM				252	252	
Alert Gap	12/13/2013	10:00 PM	12/14/2013	3:00 AM	6			
Alert processed after gap	12/14/2013	4:00 AM				245	240	
Alert Gap	12/14/2013	10:00 PM	12/15/2013	3:00 AM	6			
Alert processed after gap	12/15/2013	4:00 AM				338	332	
Alert Gap	12/15/2013	10:00 PM	12/16/2013	3:00 AM	6			
Alert processed after gap	12/16/2013	4:00 AM				267	265	
Alert Gap	12/16/2013	10:00 PM	12/17/2013	3:00 AM	6			

Alert processed after gap	12/17/2013	4:00 AM				238	238	(b)(3);6(f);b(4)
Alert Gap	12/18/2013	12:00 PM	12/18/2013	12:00 PM	1			
Alert processed after gap	12/18/2013	1:15 PM				149	149	
Alert Gap	1/11/2014	9:00 PM	1/12/2014	3:00 AM	7			
Alert processed after gap	1/12/2014	4:00 AM				176	172	
Alert Gap	1/15/2014	7:00 PM	1/15/2014	10:00 PM	4			
Alert processed after gap	1/15/2014	11:45 PM				44	44	
Alert Gap	1/16/2014	2:00 AM	1/16/2014	7:00 AM	6			
Alert processed after gap	1/16/2014	8:00 AM				178	178	
Alert Gap	1/23/2014	7:00 AM	1/23/2014	7:00 AM	1			
Alert processed after gap	1/23/2014	8:30 AM				33	33	
Alert Gap	1/25/2014	11:00 PM	1/25/2014	11:00 PM	1			
Alert processed after gap	1/26/2014	12:00 AM				11	11	
Alert Gap	1/28/2013	8:00 PM	1/29/2013	4:00 AM	9			
Alert processed after gap	1/29/2013	5:15 AM				332	332	
Alert Gap	1/31/2014	7:00 PM	2/1/2014	3:00 AM	9			
Alert processed after gap	2/1/2014	4:45 AM				24	24	
Alert Gap	2/11/2014	9:00 PM	2/12/2014	4:00 AM	8			
Alert processed after gap	2/12/2014	5:00 AM				530	530	
Alert Gap	2/13/2014	10:00 PM	2/14/2014	2:00 AM	5			
Alert processed after gap	2/14/2014	3:30 AM				167	164	
Alert Gap	2/25/2014	10:00 PM	2/26/2014	1:00 AM	4			
Alert processed after gap	2/26/2014	2:15 AM				98	98	
Alert Gap	3/13/2014	9:00 PM	3/13/2014	10:00 PM	2			
Alert processed after gap	3/13/2014	11:00 PM				71	70	

* Planned and Unplanned maintenance accounts for some portion of the gap; unable to determine the cause for the remaining time period

** Initial review of data indicates potential planned/ unplanned outage however we are unable to definitively determine

Label	Start Date	Start Time	End Date	End Time	Potential Duration (in hrs)	# of Alerts Processed	# of Members Impacted	Notes
Alert Gap	10/1/2012	12:00 AM	10/1/2012	4:00 AM	5	0		(b)(3):6(f),(b)(4)
Alert processed after gap	10/1/2012	5:45 AM				1	1	
Alert Gap	10/1/2012	7:00 PM	10/1/2012	8:00 PM	2	0		
Alert processed after gap	10/1/2012	9:00 PM				1	1	
Alert Gap	10/2/2012	2:00 AM	10/2/2012	2:00 AM	1	0		
Alert processed after gap	10/2/2012	3:00 AM				13	13	
Alert Gap	10/2/2012	5:00 AM	10/2/2012	5:00 AM	1	0		
Alert processed after gap	10/2/2012	6:15 AM				1	1	
Alert Gap	10/2/2012	4:00 PM	10/2/2012	4:00 PM	1	0		
Alert processed after gap	10/2/2012	5:00 PM				2	2	
Alert Gap	10/3/2012	2:00 AM	10/3/2012	2:00 AM	1	0		
Alert processed after gap	10/3/2012	3:30 AM				6	6	
Alert Gap	10/3/2012	4:00 AM	10/3/2012	4:00 AM	1	0		
Alert processed after gap	10/3/2012	5:45 AM				2	2	
Alert Gap	10/3/2012	7:00 PM	10/3/2012	8:00 PM	2	0		
Alert processed after gap	10/3/2012	9:00 PM				6	6	
Alert Gap	10/4/2012	2:00 AM	10/4/2012	2:00 AM	1	0		
Alert processed after gap	10/4/2012	3:30 AM				3	3	
Alert Gap	10/4/2012	5:00 AM	10/4/2012	5:00 AM	1	0		
Alert processed after gap	10/4/2012	6:15 AM				2	2	
Alert Gap	10/4/2012	8:00 PM	10/4/2012	8:00 PM	1	0		
Alert processed after gap	10/4/2012	9:00 PM				4	4	
Alert Gap	10/4/2012	10:00 PM	10/5/2012	5:00 AM	8	0		
Alert processed after gap	10/5/2012	6:15 AM				32	32	
Alert Gap	10/5/2012	10:00 AM	10/5/2012	10:00 AM	1	0		
Alert processed after gap	10/5/2012	11:00 AM				5	5	
Alert Gap	10/5/2012	5:00 PM	10/5/2012	5:00 PM	1	0		
Alert processed after gap	10/5/2012	6:15 PM				10	10	

Alert Gap	10/5/2012	7:00 PM	10/5/2012	7:00 PM	1	0	
Alert processed after gap	10/5/2012	8:00 PM				1	1
Alert Gap	10/6/2012	2:00 AM	10/6/2012	3:00 AM	2	0	
Alert processed after gap	10/6/2012	4:15 AM				6	5
Alert Gap	10/6/2012	6:00 AM	10/6/2012	6:00 AM	1	0	
Alert processed after gap	10/6/2012	7:00 AM				1	1
Alert Gap	10/6/2012	1:00 PM	10/6/2012	2:00 PM	2	0	
Alert processed after gap	10/6/2012	3:45 PM				1	1
Alert Gap	10/6/2012	8:00 PM	10/6/2012	10:00 PM	3	0	
Alert processed after gap	10/6/2012	11:00 PM				10	10
Alert Gap	10/7/2012	12:00 AM	10/7/2012	2:00 AM	3	0	
Alert processed after gap	10/7/2012	3:45 AM				1	1
Alert Gap	10/7/2012	4:00 AM	10/7/2012	4:00 AM	1	0	
Alert processed after gap	10/7/2012	5:45 AM				83	64
Alert Gap	10/7/2012	10:00 AM	10/7/2012	10:00 AM	1	0	
Alert processed after gap	10/7/2012	11:00 AM				20	18
Alert Gap	10/7/2012	1:00 PM	10/7/2012	11:00 PM	11	0	
Alert processed after gap	10/8/2012	12:00 AM				1	1
Alert Gap	10/8/2012	1:00 AM	10/8/2012	6:00 AM	6	0	
Alert processed after gap	10/8/2012	7:00 AM				3	3
Alert Gap	10/8/2012	8:00 AM	10/8/2012	8:00 AM	1	0	
Alert processed after gap	10/8/2012	9:00 AM				1	1
Alert Gap	10/8/2012	10:00 AM	10/8/2012	10:00 AM	1	0	
Alert processed after gap	10/8/2012	11:15 AM				2	2
Alert Gap	10/8/2012	1:00 PM	10/8/2012	1:00 PM	1	0	
Alert processed after gap	10/8/2012	2:30 PM				1	1
Alert Gap	10/8/2012	7:00 PM	10/8/2012	10:00 PM	4	0	
Alert processed after gap	10/8/2012	11:00 PM				40	40
Alert Gap	10/9/2012	12:00 AM	10/9/2012	5:00 AM	6	0	
Alert processed after gap	10/9/2012	6:15 AM				1	1
Alert Gap	10/9/2012	7:00 AM	10/9/2012	7:00 AM	1	0	

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

Alert processed after gap	10/9/2012	8:15 AM			1	1
Alert Gap	10/9/2012	5:00 PM	10/9/2012	5:00 PM	1	0
Alert processed after gap	10/9/2012	6:15 PM				14
Alert Gap	10/9/2012	9:00 PM	10/10/2012	5:00 AM	9	0
Alert processed after gap	10/10/2012	6:00 AM				259
Alert Gap	10/10/2012	7:00 PM	10/10/2012	8:00 PM	2	0
Alert processed after gap	10/10/2012	9:00 PM				5
Alert Gap	10/11/2012	5:00 AM	10/11/2012	5:00 AM	1	0
Alert processed after gap	10/11/2012	6:30 AM				1
Alert Gap	10/11/2012	4:00 PM	10/11/2012	5:00 PM	2	0
Alert processed after gap	10/11/2012	6:15 PM				8
Alert Gap	10/11/2012	7:00 PM	10/12/2012	6:00 AM	12	0
Alert processed after gap	10/12/2012	7:30 AM				162
Alert Gap	10/12/2012	11:00 AM	10/12/2012	11:00 AM	1	0
Alert processed after gap	10/12/2012	12:00 PM				2
Alert Gap	10/12/2012	4:00 PM	10/12/2012	4:00 PM	1	0
Alert processed after gap	10/12/2012	5:45 PM				1
Alert Gap	10/12/2012	7:00 PM	10/15/2012	7:00 AM	61	0
Alert processed after gap	10/15/2012	8:00 AM				502
Alert Gap	10/15/2012	7:00 PM	10/15/2012	7:00 PM	1	0
Alert processed after gap	10/15/2012	8:00 PM				1
Alert Gap	10/16/2012	3:00 AM	10/16/2012	3:00 AM	1	0
Alert processed after gap	10/16/2012	4:15 AM				7
Alert Gap	10/16/2012	5:00 AM	10/16/2012	5:00 AM	1	0
Alert processed after gap	10/16/2012	6:30 AM				1
Alert Gap	10/16/2012	7:00 AM	10/16/2012	7:00 AM	1	0
Alert processed after gap	10/16/2012	8:00 AM	10/16/2012			1
Alert Gap	10/16/2012	2:00 PM	10/16/2012	2:00 PM	1	0
Alert processed after gap	10/16/2012	3:00 PM				1
Alert Gap	10/16/2012	5:00 PM	10/16/2012	5:00 PM	1	0
Alert processed after gap	10/16/2012	6:15 PM				10

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

Alert Gap	10/16/2012	7:00 PM	10/16/2012	7:00 PM	1	0	
Alert processed after gap	10/16/2012	8:00 PM				2	2
Alert Gap	10/16/2012	9:00 PM	10/17/2012	5:00 AM	9	0	
Alert processed after gap	10/17/2012	6:00 AM				15	15
Alert Gap	10/17/2012	4:00 PM	10/17/2012	4:00 PM	1	0	
Alert processed after gap	10/17/2012	5:00 PM				1	1
Alert Gap	10/17/2012	7:00 PM	10/17/2012	7:00 PM	1	0	
Alert processed after gap	10/17/2012	8:15 PM				2	2
Alert Gap	10/18/2012	2:00 AM	10/18/2012	2:00 AM	1	0	
Alert processed after gap	10/18/2012	3:30 AM				7	7
Alert Gap	10/18/2012	5:00 AM	10/18/2012	5:00 AM	1	0	
Alert processed after gap	10/18/2012	6:15 AM				1	1
Alert Gap	10/18/2012	9:00 PM	10/19/2012	4:00 AM	8	0	
Alert processed after gap	10/19/2012	5:45 AM				121	121
Alert Gap	10/19/2012	7:00 AM	10/19/2012	7:00 AM	1	0	
Alert processed after gap	10/19/2012	8:15 AM				3	3
Alert Gap	10/19/2012	9:00 AM	10/19/2012	9:00 AM	1	0	
Alert processed after gap	10/19/2012	10:00 AM				1	1
Alert Gap	10/19/2012	4:00 PM	10/19/2012	4:00 PM	1	0	
Alert processed after gap	10/19/2012	5:30 PM				1	1
Alert Gap	10/19/2012	7:00 PM	10/19/2012	8:00 PM	2	0	
Alert processed after gap	10/19/2012	9:00 PM				10	10
Alert Gap	10/20/2012	11:00 AM	10/20/2012	12:00 PM	2	0	
Alert processed after gap	10/20/2012	1:15 PM				2	2
Alert Gap	10/20/2012	2:00 PM	10/20/2012	3:00 PM	2	0	
Alert processed after gap	10/20/2012	4:45 PM				1	1
Alert Gap	10/20/2012	7:00 PM	10/20/2012	7:00 PM	1	0	
Alert processed after gap	10/20/2012	8:00 PM				1	1
Alert Gap	10/20/2012	9:00 PM	10/20/2012	9:00 PM	1	0	
Alert processed after gap	10/20/2012	10:45 PM				2	2
Alert Gap	10/21/2012	12:00 AM	10/21/2012	12:00 AM	1	0	

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

Alert processed after gap	10/21/2012	1:00 AM				166	121
Alert Gap	10/21/2012	3:00 AM	10/21/2012	4:00 AM	2	0	
Alert processed after gap	10/21/2012	5:15 AM				3	3
Alert Gap	10/21/2012	8:00 AM	10/21/2012	8:00 AM	1	0	
Alert processed after gap	10/21/2012	9:15 AM				19	19
Alert Gap	10/21/2012	11:00 AM	10/21/2012	5:00 PM	7	0	
Alert processed after gap	10/21/2012	6:15 PM				1	1
Alert Gap	10/21/2012	7:00 PM	10/22/2012	5:00 AM	11	0	
Alert processed after gap	10/22/2012	6:15 AM				1	1
Alert Gap	10/22/2012	5:00 PM	10/22/2012	5:00 PM	1	0	
Alert processed after gap	10/22/2012	6:30 PM				16	16
Alert Gap	10/22/2012	7:00 PM	10/22/2012	8:00 PM	2	0	
Alert processed after gap	10/22/2012	9:00 PM				2	2
Alert Gap	10/23/2012	2:00 AM	10/23/2012	2:00 AM	1	0	
Alert processed after gap	10/23/2012	3:00 AM				4	4
Alert Gap	10/23/2012	4:00 AM	10/23/2012	6:00 AM	3	0	
Alert processed after gap	10/23/2012	7:15 AM				1	1
Alert Gap	10/23/2012	8:00 AM	10/23/2012	8:00 AM	1	0	
Alert processed after gap	10/23/2012	9:30 AM				1	1
Alert Gap	10/23/2012	12:00 PM	10/23/2012	12:00 PM	1	0	
Alert processed after gap	10/23/2012	1:15 PM				1	1
Alert Gap	10/23/2012	4:00 PM	10/23/2012	5:00 PM	2	0	
Alert processed after gap	10/23/2012	6:15 PM				10	10
Alert Gap	10/23/2012	7:00 PM	10/24/2012	5:00 AM	11	0	
Alert processed after gap	10/24/2012	6:00 AM				195	195
Alert Gap	10/24/2012	8:00 AM	10/24/2012	8:00 AM	1	0	
Alert processed after gap	10/24/2012	9:30 AM				1	1
Alert Gap	10/24/2012	5:00 PM	10/24/2012	5:00 PM	1	0	
Alert processed after gap	10/24/2012	6:00 PM				2	2
Alert Gap	10/24/2012	7:00 PM	10/24/2012	7:00 PM	1	0	
Alert processed after gap	10/24/2012	8:00 PM				1	1

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

Alert Gap	10/25/2012	5:00 AM	10/25/2012	8:00 AM	4	0	(b)(3),6(f),(b)(4)	
Alert processed after gap	10/25/2012	9:00 AM				3		3
Alert Gap	10/25/2012	3:00 PM	10/25/2012	3:00 PM	1	0		
Alert processed after gap	10/25/2012	4:15 PM				3		3
Alert Gap	10/25/2012	5:00 PM	10/25/2012	5:00 PM	1	0		
Alert processed after gap	10/25/2012	6:15 PM				6		6
Alert Gap	10/25/2012	7:00 PM	10/25/2012	7:00 PM	1	0		
Alert processed after gap	10/25/2012	8:00 PM				2		2
Alert Gap	10/25/2012	9:00 PM	10/26/2012	5:00 AM	9	0		
Alert processed after gap	10/26/2012	6:00 AM				80		80
Alert Gap	10/26/2012	2:00 PM	10/26/2012	3:00 PM	2	0		
Alert processed after gap	10/26/2012	4:15 PM				1		1
Alert Gap	10/26/2012	7:00 PM	10/26/2012	7:00 PM	1	0		
Alert processed after gap	10/26/2012	8:15 PM				1		1
Alert Gap	10/27/2012	2:00 PM	10/27/2012	5:00 PM	4	0		
Alert processed after gap	10/27/2012	6:00 PM				17		11
Alert Gap	10/27/2012	8:00 PM	10/27/2012	8:00 PM	1	0		
Alert processed after gap	10/27/2012	9:15 PM				154		124
Alert Gap	10/27/2012	10:00 PM	10/27/2012	10:00 PM	1	0		
Alert processed after gap	10/27/2012	11:00 PM				16		16
Alert Gap	10/28/2012	1:00 AM	10/28/2012	1:00 AM	1	0		
Alert processed after gap	10/28/2012	2:00 AM				359		307
Alert Gap	10/28/2012	7:00 AM	10/28/2012	7:00 AM	1	0		
Alert processed after gap	10/28/2012	8:00 AM				1		1
Alert Gap	10/28/2012	9:00 AM	10/28/2012	9:00 AM	1	0		
Alert processed after gap	10/28/2012	10:45 AM				29		24
Alert Gap	10/28/2012	12:00 PM	10/28/2012	1:00 PM	2	0		
Alert processed after gap	10/28/2012	2:15 PM				54		53
Alert Gap	10/28/2012	4:00 PM	10/28/2012	6:00 PM	3	0		
Alert processed after gap	10/28/2012	7:30 PM				2		2
Alert Gap	10/28/2012	8:00 PM	10/29/2012	7:00 AM	12	0		

Alert processed after gap	10/29/2012	8:30 AM			1	1
Alert Gap	10/29/2012	9:00 AM	10/29/2012	9:00 AM	1	0
Alert processed after gap	10/29/2012	10:45 AM			2	2
Alert Gap	10/29/2012	12:00 PM	10/29/2012	12:00 PM	1	0
Alert processed after gap	10/29/2012	1:00 PM			1	1
Alert Gap	10/29/2012	7:00 PM	10/29/2012	7:00 PM	1	0
Alert processed after gap	10/29/2012	8:00 PM			3	3
Alert Gap	10/30/2012	1:00 AM	10/30/2012	1:00 AM	1	0
Alert processed after gap	10/30/2012	2:00 AM			6	6
Alert Gap	10/30/2012	4:00 AM	10/30/2012	5:00 AM	2	0
Alert processed after gap	10/30/2012	6:45 AM			1	1
Alert Gap	10/30/2012	9:00 AM	10/30/2012	9:00 AM	1	0
Alert processed after gap	10/30/2012	10:00 AM			1	1
Alert Gap	10/30/2012	3:00 PM	10/30/2012	3:00 PM	1	0
Alert processed after gap	10/30/2012	4:15 PM			2	2
Alert Gap	10/30/2012	7:00 PM	10/30/2012	7:00 PM	1	0
Alert processed after gap	10/30/2012	8:00 PM			1	1
Alert Gap	10/30/2012	9:00 PM	10/31/2012	5:00 AM	9	0
Alert processed after gap	10/31/2012	6:00 AM			168	168
Alert Gap	10/31/2012	7:00 AM	10/31/2012	7:00 AM	1	0
Alert processed after gap	10/31/2012	8:00 AM			1	1
Alert Gap	10/31/2012	10:00 AM	10/31/2012	10:00 AM	1	0
Alert processed after gap	10/31/2012	11:00 AM			2	2
Alert Gap	10/31/2012	4:00 PM	10/31/2012	4:00 PM	1	0
Alert processed after gap	10/31/2012	5:00 PM			1	1
Alert Gap	10/31/2012	7:00 PM	10/31/2012	7:00 PM	1	0
Alert processed after gap	10/31/2012	8:00 PM			3	3
Alert Gap	11/1/2012	2:00 AM	11/1/2012	2:00 AM	1	0
Alert processed after gap	11/1/2012	3:15 AM			1	1
Alert Gap	11/1/2012	4:00 AM	11/1/2012	4:00 AM	1	0
Alert processed after gap	11/1/2012	5:00 AM			6	6

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

Alert Gap	11/1/2012	4:00 PM	11/1/2012	5:00 PM	2	0
Alert processed after gap	11/1/2012	6:15 PM				10
Alert Gap	11/1/2012	9:00 PM	11/2/2012	5:00 AM	9	0
Alert processed after gap	11/2/2012	6:00 AM				156
Alert Gap	11/2/2012	8:00 AM	11/2/2012	8:00 AM	1	0
Alert processed after gap	11/2/2012	9:45 AM				2
Alert Gap	11/2/2012	2:00 PM	11/2/2012	2:00 PM	1	0
Alert processed after gap	11/2/2012	3:45 PM				2
Alert Gap	11/2/2012	6:00 PM	11/5/2012	7:00 AM	62	0
Alert processed after gap	11/5/2012	8:00 AM				363
Alert Gap	11/5/2012	3:00 PM	11/5/2012	3:00 PM	1	0
Alert processed after gap	11/5/2012	4:00 PM				1
Alert Gap	11/5/2012	5:00 PM	11/5/2012	5:00 PM	1	0
Alert processed after gap	11/5/2012	6:45 PM				1
Alert Gap	11/5/2012	8:00 PM	11/5/2012	8:00 PM	1	0
Alert processed after gap	11/5/2012	9:30 PM				1
Alert Gap	11/6/2012	6:00 AM	11/6/2012	6:00 AM	1	0
Alert processed after gap	11/6/2012	7:00 AM				1
Alert Gap	11/6/2012	5:00 PM	11/6/2012	5:00 PM	1	0
Alert processed after gap	11/6/2012	6:15 PM				1
Alert Gap	11/6/2012	8:00 PM	11/7/2012	5:00 AM	10	0
Alert processed after gap	11/7/2012	6:00 AM				191
Alert Gap	11/7/2012	7:00 AM	11/7/2012	7:00 AM	1	0
Alert processed after gap	11/7/2012	8:00 AM				3
Alert Gap	11/7/2012	6:00 PM	11/7/2012	6:00 PM	1	0
Alert processed after gap	11/7/2012	7:15 PM				10
Alert Gap	11/7/2012	8:00 PM	11/7/2012	9:00 PM	2	0
Alert processed after gap	11/7/2012	10:00 PM				1
Alert Gap	11/8/2012	4:00 AM	11/8/2012	4:00 AM	1	0
Alert processed after gap	11/8/2012	5:30 AM				1
Alert Gap	11/8/2012	4:00 PM	11/8/2012	6:00 PM	3	0

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

Alert processed after gap	11/8/2012	7:15 PM			9	9
Alert Gap	11/8/2012	8:00 PM	11/9/2012	5:00 AM	10	0
Alert processed after gap	11/9/2012	6:15 AM			124	124
Alert Gap	11/9/2012	6:00 AM	11/12/2012	7:00 AM	62	0
Alert processed after gap	11/12/2012	8:00 AM			165	158
Alert Gap	11/12/2012	11:00 AM	11/12/2012	11:00 PM	13	0
Alert processed after gap	11/13/2012	12:00 AM			36	36
Alert Gap	11/13/2012	1:00 AM	11/13/2012	3:00 AM	3	0
Alert processed after gap	11/13/2012	4:15 AM			2	2
Alert Gap	11/13/2012	5:00 AM	11/13/2012	5:00 AM	1	0
Alert processed after gap	11/13/2012	6:30 AM			1	1
Alert Gap	11/13/2012	7:00 AM	11/13/2012	7:00 AM	1	0
Alert processed after gap	11/13/2012	8:00 AM			1	1
Alert Gap	11/13/2012	4:00 PM	11/13/2012	4:00 PM	1	0
Alert processed after gap	11/13/2012	5:15 PM			2	2
Alert Gap	11/13/2012	8:00 PM	11/14/2012	5:00 AM	10	0
Alert processed after gap	11/14/2012	6:15 AM			232	231
Alert Gap	11/15/2012	5:00 AM	11/15/2012	5:00 AM	1	0
Alert processed after gap	11/15/2012	6:00 AM			1	1
Alert Gap	11/15/2012	10:00 AM	11/15/2012	10:00 AM	1	0
Alert processed after gap	11/15/2012	11:00 AM			2	2
Alert Gap	11/15/2012	6:00 PM	11/15/2012	6:00 PM	1	0
Alert processed after gap	11/15/2012	7:15 PM			9	9
Alert Gap	11/15/2012	8:00 PM	11/16/2012	5:00 AM	10	0
Alert processed after gap	11/16/2012	6:00 AM	11/16/2012		177	175
Alert Gap	11/16/2012	5:00 PM	11/19/2012	7:00 AM	63	0
Alert processed after gap	11/19/2012	8:00 AM			506	475
Alert Gap	11/19/2012	6:00 PM	11/19/2012	6:00 PM	1	0
Alert processed after gap	11/19/2012	7:15 PM			1	1
Alert Gap	11/19/2012	8:00 PM	11/19/2012	8:00 PM	1	0
Alert processed after gap	11/19/2012	9:30 PM			1	1

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

Alert Gap	11/20/2012	4:00 AM	11/20/2012	4:00 AM	1	0	
Alert processed after gap	11/20/2012	5:00 AM				7	7
Alert Gap	11/20/2012	6:00 AM	11/20/2012	7:00 AM	2	0	
Alert processed after gap	11/20/2012	6:15 AM				1	1
Alert Gap	11/20/2012	10:00 AM	11/20/2012	10:00 AM	1	0	
Alert processed after gap	11/20/2012	11:15 AM				1	1
Alert Gap	11/20/2012	5:00 PM	11/20/2012	6:00 PM	2	0	
Alert processed after gap	11/20/2012	7:15 PM				7	7
Alert Gap	11/20/2012	8:00 PM	11/21/2012	5:00 AM	10	0	
Alert processed after gap	11/21/2012	6:00 AM				226	226
Alert Gap	11/21/2012	6:00 PM	11/21/2012	6:00 PM	1	0	
Alert processed after gap	11/21/2012	7:15 PM				10	10
Alert Gap	11/21/2012	8:00 PM	11/21/2012	8:00 PM	1	0	
Alert processed after gap	11/21/2012	9:00 PM				1	1
Alert Gap	11/22/2012	3:00 AM	11/22/2012	4:00 AM	2	0	
Alert processed after gap	11/22/2012	5:15 AM				4	4
Alert Gap	11/22/2012	6:00 AM	11/22/2012	8:00 AM	3	0	
Alert processed after gap	11/22/2012	9:15 AM				2	2
Alert Gap	11/22/2012	10:00 AM	11/22/2012	1:00 PM	4	0	
Alert processed after gap	11/22/2012	2:30 PM				1	1
Alert Gap	11/22/2012	3:00 PM	11/22/2012	5:00 PM	3	0	
Alert processed after gap	11/22/2012	6:30 PM				1	1
Alert Gap	11/22/2012	7:00 PM	11/22/2012	11:00 PM	5	0	
Alert processed after gap	11/23/2012	12:00 AM				30	30
Alert Gap	11/23/2012	1:00 AM	11/23/2012	8:00 AM	8	0	
Alert processed after gap	11/23/2012	9:15 AM				1	1
Alert Gap	11/23/2012	5:00 PM	11/26/2012	7:00 AM	63	0	
Alert processed after gap	11/26/2012	8:00 AM				234	220
Alert Gap	11/26/2012	5:00 PM	11/26/2012	6:00 PM	2	0	
Alert processed after gap	11/26/2012	7:15 PM				14	14
Alert Gap	11/26/2012	8:00 PM	11/26/2012	8:00 PM	1	0	

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

Alert processed after gap	11/26/2012	9:00 PM			1	1
Alert Gap	11/27/2012	3:00 AM	11/27/2012	3:00 AM	1	0
Alert processed after gap	11/27/2012	4:00 AM			2	2
Alert Gap	11/27/2012	6:00 AM	11/27/2012	6:00 AM	1	0
Alert processed after gap	11/27/2012	7:00 AM			1	1
Alert Gap	11/27/2012	5:00 PM	11/27/2012	5:00 PM	1	0
Alert processed after gap	11/27/2012	6:15 PM			1	1
Alert Gap	11/27/2012	9:00 PM	11/28/2012	5:00 AM	9	0
Alert processed after gap	11/28/2012	6:00 AM			212	212
Alert Gap	11/28/2012	7:00 AM	11/28/2012	7:00 AM	1	0
Alert processed after gap	11/28/2012	8:30 AM			2	2
Alert Gap	11/28/2012	9:00 AM	11/28/2012	9:00 AM	1	0
Alert processed after gap	11/28/2012	10:00 AM			1	1
Alert Gap	11/28/2012	12:00 PM	11/28/2012	12:00 PM	1	0
Alert processed after gap	11/28/2012	1:45 PM			1	1
Alert Gap	11/28/2012	3:00 PM	11/28/2012	3:00 PM	1	0
Alert processed after gap	11/28/2012	4:00 PM			1	1
Alert Gap	11/28/2012	6:00 PM	11/28/2012	6:00 PM	1	0
Alert processed after gap	11/28/2012	7:15 PM			6	6
Alert Gap	11/28/2012	8:00 PM	11/28/2012	9:00 PM	2	0
Alert processed after gap	11/28/2012	10:00 PM			1	1
Alert Gap	11/29/2012	5:00 AM	11/29/2012	5:00 AM	1	0
Alert processed after gap	11/29/2012	6:30 AM			2	2
Alert Gap	11/29/2012	8:00 AM	11/29/2012	8:00 AM	1	0
Alert processed after gap	11/29/2012	9:00 AM			1	1
Alert Gap	11/29/2012	6:00 PM	11/29/2012	6:00 PM	1	0
Alert processed after gap	11/29/2012	7:15 PM			5	5
Alert Gap	11/29/2012	8:00 PM	11/30/2012	5:00 AM	10	0
Alert processed after gap	11/30/2012	6:15 AM			171	171
Alert Gap	11/30/2012	6:00 PM	12/3/2012	7:00 AM	62	0
Alert processed after gap	12/3/2012	8:00 AM			315	291

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

Alert Gap	12/3/2012	5:00 PM	12/3/2012	6:00 PM	2	0
Alert processed after gap	12/3/2012	7:15 PM				13
Alert Gap	12/3/2012	8:00 PM	12/3/2012	9:00 PM	2	0
Alert processed after gap	12/3/2012	10:00 AM				2
Alert Gap	12/4/2012	1:00 AM	12/4/2012	1:00 AM	1	0
Alert processed after gap	12/4/2012	2:15 AM				12
Alert Gap	12/4/2012	6:00 AM	12/4/2012	6:00 AM	1	0
Alert processed after gap	12/4/2012	7:45 AM				1
Alert Gap	12/4/2012	5:00 PM	12/4/2012	5:00 PM	1	0
Alert processed after gap	12/4/2012	6:30 PM				4
Alert Gap	12/4/2012	8:00 PM	12/5/2012	12:00 PM	17	0
Alert processed after gap	12/5/2012	1:00 PM				251
Alert Gap	12/5/2012	6:00 PM	12/5/2012	6:00 PM	1	0
Alert processed after gap	12/5/2012	7:15 PM				12
Alert Gap	12/5/2012	8:00 PM	12/5/2012	9:00 PM	2	0
Alert processed after gap	12/5/2012	10:00 PM				3
Alert Gap	12/6/2012	2:00 AM	12/6/2012	2:00 AM	1	0
Alert processed after gap	12/6/2012	3:15 PM				1
Alert Gap	12/6/2012	5:00 PM	12/6/2012	6:00 PM	2	0
Alert processed after gap	12/6/2012	7:00 AM				2
Alert Gap	12/6/2012	6:00 PM	12/6/2012	6:00 PM	1	0
Alert processed after gap	12/6/2012	7:00 PM				1
Alert Gap	12/7/2012	3:00 AM	12/7/2012	3:00 AM	1	0
Alert processed after gap	12/7/2012	4:30 AM				9
Alert Gap	12/7/2012	6:00 AM	12/7/2012	7:00 AM	2	0
Alert processed after gap	12/7/2012	8:00 AM				2
Alert Gap	12/7/2012	6:00 PM	12/10/2012	8:00 AM	63	0
Alert processed after gap	12/10/2012	9:15 AM				444
Alert Gap	12/10/2012	6:00 PM	12/10/2012	6:00 PM	1	0
Alert processed after gap	12/10/2012	7:15 PM				26
Alert Gap	12/10/2012	8:00 PM	12/10/2012	9:00 PM	2	0

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

Alert processed after gap	12/10/2012	10:00 PM			3	3
Alert Gap	12/11/2012	3:00 AM	12/11/2012	3:00 AM	1	0
Alert processed after gap	12/11/2012	4:30 AM			10	10
Alert Gap	12/11/2012	6:00 AM	12/11/2012	6:00 AM	1	0
Alert processed after gap	12/11/2012	7:15 AM			2	2
Alert Gap	12/11/2012	4:00 PM	12/11/2012	4:00 PM	1	0
Alert processed after gap	12/11/2012	5:15 PM			1	1
Alert Gap	12/11/2012	6:00 PM	12/11/2012	6:00 PM	1	0
Alert processed after gap	12/11/2012	7:15 PM			13	13
Alert Gap	12/11/2012	8:00 PM	12/12/2012	5:00 AM	10	0
Alert processed after gap	12/12/2012	6:00 AM			6	6
Alert Gap	12/12/2012	6:00 PM	12/12/2012	6:00 PM	1	0
Alert processed after gap	12/12/2012	7:00 PM			1	1
Alert Gap	12/12/2012	8:00 PM	12/12/2012	8:00 PM	1	0
Alert processed after gap	12/12/2012	9:00 PM			3	3
Alert Gap	12/13/2012	3:00 AM	12/13/2012	4:00 AM	1	0
Alert processed after gap	12/13/2012	5:00 AM			11	11
Alert Gap	12/13/2012	4:00 PM	12/13/2012	4:00 PM	1	0
Alert processed after gap	12/13/2012	5:30 PM			1	1
Alert Gap	12/13/2012	8:00 PM	12/14/2012	6:00 AM	11	0
Alert processed after gap	12/14/2012	7:45 AM			171	171
Alert Gap	12/14/2012	6:00 PM	12/17/2012	7:00 AM	62	0
Alert processed after gap	12/17/2012	8:00 AM			353	347
Alert Gap	12/17/2012	8:00 PM	12/17/2012	9:00 PM	2	0
Alert processed after gap	12/17/2012	10:00 PM			2	2
Alert Gap	12/18/2012	5:00 AM	12/18/2012	6:00 AM	2	0
Alert processed after gap	12/18/2012	7:00 AM			1	1
Alert Gap	12/18/2012	6:00 PM	12/18/2012	6:00 PM	1	0
Alert processed after gap	12/18/2012	7:15 PM			8	8
Alert Gap	12/18/2012	8:00 PM	12/18/2012	9:00 PM	2	0
Alert processed after gap	12/18/2012	10:00 PM			1	1

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

Alert Gap	12/19/2012	6:00 AM	12/19/2012	6:00 AM	1	0	(b)(3);6(f),(b)(4)	
Alert processed after gap	12/19/2012	7:00 AM				1		1
Alert Gap	12/19/2012	4:00 PM	12/19/2012	5:00 PM	2	0		
Alert processed after gap	12/19/2012	6:00 PM				1		1
Alert Gap	12/19/2012	8:00 PM	12/19/2012	9:00 PM	2	0		
Alert processed after gap	12/19/2012	10:00 PM				2		2
Alert Gap	12/20/2012	1:00 AM	12/20/2012	1:00 AM	1	0		
Alert processed after gap	12/20/2012	2:00 AM				9		9
Alert Gap	12/20/2012	3:00 AM	12/20/2012	3:00 AM	1	0		
Alert processed after gap	12/20/2012	4:00 AM				2		2
Alert Gap	12/20/2012	5:00 AM	12/20/2012	5:00 AM	1	0		
Alert processed after gap	12/20/2012	6:30 AM				1		1
Alert Gap	12/20/2012	8:00 PM	12/20/2012	9:00 PM	2	0		
Alert processed after gap	12/20/2012	10:00 PM				1		1
Alert Gap	12/21/2012	3:00 AM	12/21/2012	3:00 AM	1	0		
Alert processed after gap	12/21/2012	4:30 AM				6		6
Alert Gap	12/21/2012	6:00 AM	12/21/2012	6:00 AM	1	0		
Alert processed after gap	12/21/2012	7:15 AM				1		1
Alert Gap	12/21/2012	5:00 PM	12/24/2012	7:00 AM	63	0		
Alert processed after gap	12/24/2012	8:00 AM				302		265
Alert Gap	12/24/2012	4:00 PM	12/24/2012	6:00 PM	3	0		
Alert processed after gap	12/24/2012	7:15 PM				7		7
Alert Gap	12/24/2012	8:00 PM	12/24/2012	9:00 PM	2	0		
Alert processed after gap	12/24/2012	10:00 PM				2		2
Alert Gap	12/25/2012	5:00 AM	12/25/2012	11:00 AM	7	0		
Alert processed after gap	12/25/2012	12:30 PM				1		1
Alert Gap	12/25/2012	1:00 PM	12/25/2012	11:00 PM	11	0		
Alert processed after gap	12/26/2012	12:00 AM				46		46
Alert Gap	12/26/2012	1:00 AM	12/26/2012	7:00 AM	7	0		
Alert processed after gap	12/26/2012	8:00 AM				3		3
Alert Gap	12/26/2012	4:00 PM	12/26/2012	4:00 PM	1	0		

Alert processed after gap	12/26/2012	5:30 PM			2	2
Alert Gap	12/26/2012	6:00 PM	12/26/2012	6:00 PM	1	0
Alert processed after gap	12/26/2012	7:15 PM			13	13
Alert Gap	12/26/2012	8:00 PM	12/26/2012	9:00 PM	2	0
Alert processed after gap	12/26/2012	10:00 PM			2	2
Alert Gap	12/27/2012	2:00 AM	12/27/2012	3:00 AM	2	0
Alert processed after gap	12/27/2012	4:30 AM			7	7
Alert Gap	12/27/2012	5:00 AM	12/27/2012	6:00 AM	2	0
Alert processed after gap	12/27/2012	7:30 AM			1	1
Alert Gap	12/27/2012	6:00 PM	12/27/2012	6:00 PM	1	0
Alert processed after gap	12/27/2012	7:15 PM			19	19
Alert Gap	12/27/2012	8:00 PM	12/27/2012	8:00 PM	1	0
Alert processed after gap	12/27/2012	9:00 PM			1	1
Alert Gap	12/28/2012	2:00 AM	12/28/2012	3:00 AM	2	0
Alert processed after gap	12/28/2012	4:00 AM			1	1
Alert Gap	12/28/2012	5:00 AM	12/28/2012	5:00 AM	1	0
Alert processed after gap	12/28/2012	6:00 AM			9	9
Alert Gap	12/28/2012	7:00 AM	12/28/2012	7:00 AM	1	0
Alert processed after gap	12/28/2012	8:30 AM			2	2
Alert Gap	12/28/2012	9:00 AM	12/28/2012	9:00 AM	1	0
Alert processed after gap	12/28/2012	10:00 AM			2	2
Alert Gap	12/28/2012	6:00 PM	12/31/2012	7:00 AM	62	0
Alert processed after gap	12/31/2012	8:00 AM			371	331
Alert Gap	12/31/2012	5:00 AM	12/31/2012	6:00 AM	2	0
Alert processed after gap	12/31/2012	7:15 PM			23	23
Alert Gap	12/31/2012	8:00 PM	12/31/2012	8:00 PM	1	0
Alert processed after gap	12/31/2012	9:00 PM			2	2
Alert Gap	1/1/2013	3:00 AM	1/1/2013	3:00 AM	1	0
Alert processed after gap	1/1/2013	4:00 AM			1	1
Alert Gap	1/1/2013	6:00 AM	1/1/2013	7:00 AM	2	0
Alert processed after gap	1/1/2013	8:30 AM			1	1

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

Alert Gap	1/1/2013	9:00 AM	1/1/2013	10:00 AM	2	0		
Alert processed after gap	1/1/2013	11:00 AM				1	1	
Alert Gap	1/1/2013	1:00 PM	1/1/2013	11:00 PM	11	0		
Alert processed after gap	1/2/2013	12:00 AM				3	3	
Alert Gap	1/2/2013	2:00 AM	1/2/2013	4:00 AM	3	0		
Alert processed after gap	1/2/2013	5:15 AM				1	1	
Alert Gap	1/3/2013	3:00 AM	1/3/2013	3:00 AM	1	0		
Alert processed after gap	1/3/2013	4:00 AM				3	3	
Alert Gap	1/3/2013	5:00 AM	1/3/2013	5:00 AM	1	0		
Alert processed after gap	1/3/2013	6:45 AM				1	1	
Alert Gap	1/3/2013	8:00 PM	1/4/2013	5:00 AM	10	0		
Alert processed after gap	1/4/2013	6:00 AM				13	13	
Alert Gap	1/4/2013	6:00 PM	1/7/2013	7:00 AM	62	0		
Alert processed after gap	1/7/2013	8:00 AM				425	384	
Alert Gap	1/7/2013	8:00 PM	1/7/2013	8:00 PM	1	0		
Alert processed after gap	1/7/2013	9:00 PM				1	1	
Alert Gap	1/8/2013	6:00 AM	1/8/2013	6:00 AM	1	0		
Alert processed after gap	1/8/2013	7:15 AM				2	2	
Alert Gap	1/8/2013	5:00 PM	1/8/2013	5:00 PM	1	0		
Alert processed after gap	1/8/2013	6:00 PM				2	2	
Alert Gap	1/8/2013	8:00 PM	1/9/2013	5:00 AM	10	0		
Alert processed after gap	1/9/2013	6:00 AM				22	22	
Alert Gap	1/9/2013	4:00 PM	1/9/2013	4:00 PM	1	0		
Alert processed after gap	1/9/2013	5:15 PM				1	1	
Alert Gap	1/9/2013	8:00 PM	1/9/2013	8:00 PM	1	0		
Alert processed after gap	1/9/2013	9:00 PM				1	1	
Alert Gap	1/10/2013	2:00 AM	1/10/2013	2:00 AM	1	0		
Alert processed after gap	1/10/2013	3:00 AM				8	8	
Alert Gap	1/10/2013	5:00 AM	1/10/2013	5:00 AM	1	0		
Alert processed after gap	1/10/2013	6:15 AM				1	1	
Alert Gap	1/10/2013	8:00 PM	1/11/2013	5:00 AM	10	0		

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

Alert processed after gap	1/11/2013	6:00 AM				20	20
Alert Gap	1/11/2013	12:00 PM	1/11/2013	12:00 PM	1	0	
Alert processed after gap	1/11/2013	1:00 PM				3	3
Alert Gap	1/11/2013	6:00 PM	1/14/2013	7:00 AM	62	0	
Alert processed after gap	1/14/2013	8:00 AM				343	319
Alert Gap	1/14/2013	8:00 PM	1/14/2013	8:00 PM	1	0	
Alert processed after gap	1/14/2013	9:00 PM				2	2
Alert Gap	1/15/2013	5:00 AM	1/15/2013	6:00 AM	2	0	
Alert processed after gap	1/15/2013	7:00 AM				1	1
Alert Gap	1/15/2013	5:00 PM	1/15/2013	6:00 PM	2	0	
Alert processed after gap	1/15/2013	7:15 PM				18	18
Alert Gap	1/15/2013	8:00 PM	1/15/2013	9:00 PM	2	0	
Alert processed after gap	1/15/2013	10:00 PM				2	2
Alert Gap	1/16/2013	12:00 AM	1/16/2013	5:00 AM	6	0	
Alert processed after gap	1/16/2013	6:00 AM				21	21
Alert Gap	1/16/2013	6:00 PM	1/16/2013	6:00 PM	1	0	
Alert processed after gap	1/16/2013	7:00 PM				2	2
Alert Gap	1/16/2013	8:00 PM	1/16/2013	9:00 PM	2	0	
Alert processed after gap	1/16/2013	10:00 PM				1	1
Alert Gap	1/17/2013	6:00 AM	1/17/2013	6:00 AM	1	0	
Alert processed after gap	1/17/2013	7:45 AM				1	1
Alert Gap	1/17/2013	1:00 PM	1/17/2013	1:00 PM	1	0	
Alert processed after gap	1/17/2013	2:30 PM				1	1
Alert Gap	1/17/2013	4:00 PM	1/17/2013	4:00 PM	1	0	
Alert processed after gap	1/17/2013	5:15 PM				1	1
Alert Gap	1/17/2013	9:00 PM	1/18/2013	5:00 AM	9	0	
Alert processed after gap	1/18/2013	6:00 AM				6	6
Alert Gap	1/18/2013	6:00 PM	1/21/2013	7:00 AM	62	0	
Alert processed after gap	1/21/2013	8:00 AM				374	334
Alert Gap	1/21/2013	10:00 AM	1/21/2013	11:00 AM	2	0	
Alert processed after gap	1/21/2013	12:00 PM				1	1

(b)(3);6(f);b(4)

Alert Gap	1/21/2013	2:00 PM	1/21/2013	3:00 PM	2	0
Alert processed after gap	1/21/2013	4:45 PM				1
Alert Gap	1/21/2013	5:00 PM	1/21/2013	11:00 PM	7	0
Alert processed after gap	1/22/2013	12:00 AM				13
Alert Gap	1/22/2013	1:00 AM	1/22/2013	3:00 AM	3	0
Alert processed after gap	1/22/2013	4:00 AM				2
Alert Gap	1/22/2013	5:00 AM	1/22/2013	7:00 AM	3	0
Alert processed after gap	1/22/2013	8:45 AM				1
Alert Gap	1/22/2013	8:00 PM	1/22/2013	8:00 PM	1	0
Alert processed after gap	1/22/2013	9:00 PM				1
Alert Gap	1/22/2013	11:00 PM	1/23/2013	5:00 AM	6	0
Alert processed after gap	1/23/2013	6:00 AM				313
Alert Gap	1/23/2013	7:00 AM	1/23/2013	7:00 AM	1	0
Alert processed after gap	1/23/2013	8:00 AM				3
Alert Gap	1/23/2013	6:00 PM	1/23/2013	6:00 PM	1	0
Alert processed after gap	1/23/2013	7:15 PM				20
Alert Gap	1/23/2013	8:00 PM	1/23/2013	8:00 PM	1	0
Alert processed after gap	1/23/2013	9:30 PM				1
Alert Gap	1/24/2013	1:00 AM	1/24/2013	1:00 AM	1	0
Alert processed after gap	1/24/2013	2:00 AM				15
Alert Gap	1/24/2013	6:00 PM	1/24/2013	6:00 PM	1	0
Alert processed after gap	1/24/2013	7:15 PM				14
Alert Gap	1/24/2013	8:00 PM	1/25/2013	8:00 PM	13	0
Alert processed after gap	1/25/2013	9:00 AM				209
Alert Gap	1/25/2013	5:00 PM	1/28/2013	7:00 AM	63	0
Alert processed after gap	1/28/2013	8:00 AM				88
Alert Gap	1/28/2013	8:00 PM	1/29/2013	5:00 AM	10	0
Alert processed after gap	1/29/2013	6:00 AM				281
Alert Gap	1/29/2013	8:00 PM	1/29/2013	9:00 PM	2	0
Alert processed after gap	1/29/2013	10:15 PM				2
Alert Gap	1/29/2013	11:00 PM	1/30/2013	4:00 AM	6	0

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

Alert processed after gap	1/30/2013	5:15 AM				164	164
Alert Gap	1/30/2013	6:00 AM	1/30/2013	6:00 AM	1	0	
Alert processed after gap	1/30/2013	7:30 AM				1	1
Alert Gap	1/30/2013	8:00 AM	1/30/2013	10:00 AM	3	0	
Alert processed after gap	1/30/2013	11:15 AM				11	11
Alert Gap	1/30/2013	5:00 PM	1/30/2013	5:00 PM	1	0	
Alert processed after gap	1/30/2013	6:15 PM				1	1
Alert Gap	1/30/2013	8:00 PM	1/30/2013	8:00 PM	1	0	
Alert processed after gap	1/30/2013	9:15 PM				2	2
Alert Gap	1/31/2013	5:00 AM	1/31/2013	5:00 AM	1	0	
Alert processed after gap	1/31/2013	6:15 AM				5	5
Alert Gap	1/31/2013	9:00 AM	1/31/2013	9:00 AM	1	0	
Alert processed after gap	1/31/2013	10:00 AM				1	1
Alert Gap	1/31/2013	9:00 PM	2/1/2013	5:00 AM	9	0	
Alert processed after gap	2/1/2013	6:00 AM				198	196
Alert Gap	2/1/2013	4:00 PM	2/1/2013	4:00 PM	1	0	
Alert processed after gap	2/1/2013	5:00 PM				2	2
Alert Gap	2/1/2013	6:00 PM	2/4/2013	7:00 AM	62	0	
Alert processed after gap	2/4/2013	8:00 AM				439	411
Alert Gap	2/4/2013	6:00 PM	2/4/2013	6:00 PM	1	0	
Alert processed after gap	2/4/2013	7:15 PM				24	24
Alert Gap	2/4/2013	8:00 PM	2/4/2013	9:00 PM	2	0	
Alert processed after gap	2/4/2013	10:00 PM				3	3
Alert Gap	2/5/2013	1:00 AM	2/5/2013	1:00 AM	1	0	
Alert processed after gap	2/5/2013	2:00 AM				11	11
Alert Gap	2/5/2013	5:00 AM	2/5/2013	5:00 AM	1	0	
Alert processed after gap	2/5/2013	6:30 AM				2	2
Alert Gap	2/5/2013	5:00 PM	2/5/2013	5:00 PM	1	0	
Alert processed after gap	2/5/2013	6:15 PM				1	1
Alert Gap	2/5/2013	8:00 PM	2/5/2013	9:00 PM	2	0	
Alert processed after gap	2/5/2013	10:00 PM				1	1

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

Alert Gap	2/6/2013	3:00 AM	2/6/2013	3:00 AM	1	0	
Alert processed after gap	2/6/2013	4:30 AM				4	4
Alert Gap	2/6/2013	5:00 AM	2/6/2013	5:00 AM	1	0	
Alert processed after gap	2/6/2013	6:00 AM				1	1
Alert Gap	2/6/2013	8:00 PM	2/6/2013	9:00 PM	2	0	
Alert processed after gap	2/6/2013	10:00 PM				3	3
Alert Gap	2/7/2013	4:00 AM	2/7/2013	4:00 AM	1	0	
Alert processed after gap	2/7/2013	5:00 AM				3	3
Alert Gap	2/7/2013	6:00 AM	2/7/2013	6:00 AM	1	0	
Alert processed after gap	2/7/2013	7:00 AM				6	6
Alert Gap	2/8/2013	4:00 AM	2/8/2013	4:00 AM	1	0	
Alert processed after gap	2/8/2013	5:30 AM				1	1
Alert Gap	2/8/2013	4:00 PM	2/8/2013	4:00 PM	1	0	
Alert processed after gap	2/8/2013	5:30 PM				1	1
Alert Gap	2/8/2013	6:00 PM	2/11/2013	7:00 AM	62	0	
Alert processed after gap	2/11/2013	8:00 AM				522	473
Alert Gap	2/11/2013	5:00 PM	2/11/2013	5:00 PM	1	0	
Alert processed after gap	2/11/2013	6:30 PM				1	1
Alert Gap	2/11/2013	8:00 PM	2/11/2013	9:00 PM	2	0	
Alert processed after gap	2/11/2013	10:30 PM				4	4
Alert Gap	2/12/2013	9:00 PM	2/13/2013	5:00 AM	9	0	
Alert processed after gap	2/13/2013	6:15 AM				274	274
Alert Gap	2/13/2013	5:00 PM	2/13/2013	5:00 PM	1	0	
Alert processed after gap	2/13/2013	6:45 PM				1	1
Alert Gap	2/13/2013	8:00 PM	2/13/2013	8:00 PM	1	0	
Alert processed after gap	2/13/2013	9:00 PM				1	1
Alert Gap	2/14/2013	6:00 AM	2/14/2013	6:00 AM	1	0	
Alert processed after gap	2/14/2013	7:45 AM				2	2
Alert Gap	2/14/2013	4:00 PM	2/14/2013	4:00 PM	1	0	
Alert processed after gap	2/14/2013	5:00 PM				1	1
Alert Gap	2/14/2013	9:00 PM	2/15/2013	7:00 AM	11	0	

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

Alert processed after gap	2/15/2013	8:00 AM			213	213
Alert Gap	2/15/2013	6:00 PM	2/18/2013	7:00 AM	62	0
Alert processed after gap	2/18/2013	8:00 AM			512	475
Alert Gap	2/18/2013	3:00 PM	2/18/2013	3:00 PM	1	0
Alert processed after gap	2/18/2013	4:45 PM			1	1
Alert Gap	2/18/2013	6:00 PM	2/18/2013	7:00 PM	2	0
Alert processed after gap	2/18/2013	8:00 PM			1	1
Alert Gap	2/18/2013	9:00 PM	2/18/2013	11:00 PM	3	0
Alert processed after gap	2/19/2013	12:00 AM			5	5
Alert Gap	2/19/2013	1:00 AM	2/19/2013	3:00 AM	3	0
Alert processed after gap	2/19/2013	4:15 AM			5	5
Alert Gap	2/19/2013	5:00 AM	2/19/2013	7:00 AM	3	0
Alert processed after gap	2/19/2013	8:15 AM			1	1
Alert Gap	2/20/2013	5:00 AM	2/20/2013	5:00 AM	1	0
Alert processed after gap	2/20/2013	6:15 AM			6	6
Alert Gap	2/20/2013	6:00 PM	2/20/2013	6:00 PM	1	0
Alert processed after gap	2/20/2013	7:15 PM			14	14
Alert Gap	2/20/2013	8:00 PM	2/20/2013	9:00 PM	2	0
Alert processed after gap	2/20/2013	10:00 PM			2	2
Alert Gap	2/21/2013	2:00 AM	2/21/2013	2:00 AM	1	0
Alert processed after gap	2/21/2013	3:15 AM			1	1
Alert Gap	2/21/2013	6:00 AM	2/21/2013	6:00 AM	1	0
Alert processed after gap	2/21/2013	7:00 AM			2	2
Alert Gap	2/21/2013	8:00 PM	2/22/2013	4:00 AM	9	0
Alert processed after gap	2/22/2013	5:45 AM			78	78
Alert Gap	2/22/2013	6:00 PM	2/25/2013	7:00 AM	62	0
Alert processed after gap	2/25/2013	8:00 AM			355	299
Alert Gap	2/25/2013	6:00 PM	2/25/2013	6:00 PM	1	0
Alert processed after gap	2/25/2013	7:15 PM			18	18
Alert Gap	2/25/2013	8:00 PM	2/25/2013	8:00 PM	1	0

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

Alert processed after gap	2/25/2013	9:00 PM			1	1
Alert Gap	2/26/2013	3:00 AM	2/26/2013	3:00 AM	1	0
Alert processed after gap	2/26/2013	4:00 AM			1	1
Alert Gap	2/26/2013	5:00 PM	2/26/2013	6:00 PM	2	0
Alert processed after gap	2/26/2013	7:15 PM			11	11
Alert Gap	2/26/2013	8:00 PM	2/27/2013	8:00 AM	13	0
Alert processed after gap	2/27/2013	9:00 AM			18	18
Alert Gap	2/27/2013	8:00 PM	2/27/2013	8:00 PM	1	0
Alert processed after gap	2/27/2013	9:00 PM			4	4
Alert Gap	2/28/2013	4:00 AM	2/28/2013	4:00 AM	1	0
Alert processed after gap	2/28/2013	5:30 AM			5	5
Alert Gap	2/28/2013	8:00 PM	2/28/2013	8:00 PM	1	0
Alert processed after gap	2/28/2013	9:15 PM			2	2
Alert Gap	3/1/2013	3:00 AM	3/1/2013	3:00 AM	1	0
Alert processed after gap	3/1/2013	4:45 AM			1	1
Alert Gap	3/1/2013	6:00 PM	3/4/2013	7:00 AM	62	0
Alert processed after gap	3/4/2013	8:00 AM			167	157
Alert Gap	3/4/2013	6:00 PM	3/4/2013	6:00 PM	1	0
Alert processed after gap	3/4/2013	7:15 PM			29	29
Alert Gap	3/4/2013	8:00 PM	3/4/2013	8:00 PM	1	0
Alert processed after gap	3/4/2013	9:00 PM			1	1
Alert Gap	3/5/2013	3:00 AM	3/5/2013	3:00 AM	1	0
Alert processed after gap	3/5/2013	4:15 AM	3/5/2013		4	4
Alert Gap	3/5/2013	5:00 AM	3/5/2013	5:00 AM	1	0
Alert processed after gap	3/5/2013	6:15 AM			1	1
Alert Gap	3/5/2013	3:00 PM	3/5/2013	3:00 PM	1	0
Alert processed after gap	3/5/2013	4:30 PM			6	6
Alert Gap	3/5/2013	8:00 PM	3/5/2013	8:00 PM	1	0
Alert processed after gap	3/5/2013	9:00 PM			1	1
Alert Gap	3/6/2013	4:00 AM	3/6/2013	5:00 AM	2	0
Alert processed after gap	3/6/2013	6:15 AM			1	1

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

Alert Gap	3/6/2013	7:00 AM	3/6/2013	7:00 AM	1	0	
Alert processed after gap	3/6/2013	8:30 AM				1	1
Alert Gap	3/6/2013	8:00 PM	3/6/2013	9:00 PM	2	0	
Alert processed after gap	3/6/2013	10:00 PM				2	2
Alert Gap	3/7/2013	2:00 AM	3/7/2013	2:00 AM	1	0	
Alert processed after gap	3/7/2013	3:15 AM				3	3
Alert Gap	3/7/2013	4:00 AM	3/7/2013	4:00 AM	1	0	
Alert processed after gap	3/7/2013	5:30 AM				4	4
Alert Gap	3/7/2013	6:00 AM	3/7/2013	6:00 AM	1	0	
Alert processed after gap	3/7/2013	7:00 AM				1	1
Alert Gap	3/7/2013	9:00 PM	3/8/2013	5:00 AM	9	0	
Alert processed after gap	3/8/2013	6:15 AM				191	191
Alert Gap	3/8/2013	6:00 PM	3/11/2013	7:00 AM	62	0	
Alert processed after gap	3/11/2013	8:00 AM				166	149
Alert Gap	3/11/2013	7:00 PM	3/11/2013	7:00 PM	1	0	
Alert processed after gap	3/11/2013	8:00 PM				1	1
Alert Gap	3/12/2013	2:00 AM	3/12/2013	2:00 AM	1	0	
Alert processed after gap	3/12/2013	3:00 AM				9	9
Alert Gap	3/12/2013	5:00 AM	3/12/2013	5:00 AM	1	0	
Alert processed after gap	3/12/2013	6:15 AM				1	1
Alert Gap	3/12/2013	5:00 PM	3/13/2013	5:00 AM	13	0	
Alert processed after gap	3/13/2013	6:00 AM				264	263
Alert Gap	3/13/2013	7:00 PM	3/13/2013	7:00 PM	1	0	
Alert processed after gap	3/13/2013	8:00 PM				2	2
Alert Gap	3/14/2013	1:00 AM	3/14/2013	1:00 AM	1	0	
Alert processed after gap	3/14/2013	2:15 AM				1	1
Alert Gap	3/14/2013	5:00 AM	3/14/2013	5:00 AM	1	0	
Alert processed after gap	3/14/2013	6:00 AM				1	1
Alert Gap	3/14/2013	1:00 PM	3/14/2013	1:00 PM	1	0	
Alert processed after gap	3/14/2013	2:15 PM				2	2
Alert Gap	3/14/2013	7:00 PM	3/15/2013	5:00 AM	11	0	

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

Alert processed after gap	3/15/2013	6:00 AM				238	238
Alert Gap	3/15/2013	6:00 PM	3/18/2013	6:00 AM	61	0	
Alert processed after gap	3/18/2013	7:45 AM				85	80
Alert Gap	3/18/2013	7:00 PM	3/18/2013	7:00 PM	1	0	
Alert processed after gap	3/18/2013	8:00 PM				1	1
Alert Gap	3/19/2013	2:00 AM	3/19/2013	2:00 AM	1	0	
Alert processed after gap	3/19/2013	3:00 AM				5	5
Alert Gap	3/19/2013	5:00 AM	3/19/2013	5:00 AM	1	0	
Alert processed after gap	3/19/2013	6:00 AM				2	2
Alert Gap	3/19/2013	7:00 PM	3/20/2013	5:00 AM	11	0	
Alert processed after gap	3/20/2013	6:00 AM				286	286
Alert Gap	3/20/2013	8:00 AM	3/20/2013	8:00 AM	1	0	
Alert processed after gap	3/20/2013	9:00 AM				3	3
Alert Gap	3/20/2013	7:00 PM	3/20/2013	7:00 PM	1	0	
Alert processed after gap	3/20/2013	8:00 PM				1	1
Alert Gap	3/20/2013	9:00 PM	3/21/2013	5:00 AM	9	0	
Alert processed after gap	3/21/2013	6:00 AM				237	237
Alert Gap	3/21/2013	5:00 PM	3/21/2013	5:00 PM	1	0	
Alert processed after gap	3/21/2013	6:00 PM				15	15
Alert Gap	3/21/2013	9:00 PM	3/22/2013	5:00 AM	9	0	
Alert processed after gap	3/22/2013	6:00 AM				20	20
Alert Gap	3/22/2013	4:00 PM	3/22/2013	4:00 PM	1	0	
Alert processed after gap	3/22/2013	5:30 PM				1	1
Alert Gap	3/22/2013	6:00 PM	3/25/2013	7:00 AM	62	0	
Alert processed after gap	3/25/2013	8:00 AM				480	455
Alert Gap	3/25/2013	7:00 PM	3/25/2013	7:00 PM	1	0	
Alert processed after gap	3/25/2013	8:00 PM				1	1
Alert Gap	3/26/2013	6:00 AM	3/26/2013	6:00 AM	1	0	
Alert processed after gap	3/26/2013	7:00 AM				2	2
Alert Gap	3/26/2013	9:00 PM	3/27/2013	5:00 AM	9	0	
Alert processed after gap	3/27/2013	6:15 AM				104	104

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

Alert Gap	3/27/2013	11:00 AM	3/27/2013	1:00 PM	3	0	
Alert processed after gap	3/27/2013	2:45 PM				24	24
Alert Gap	3/27/2013	5:00 PM	3/27/2013	5:00 PM	1	0	
Alert processed after gap	3/27/2013	6:00 PM				1	1
Alert Gap	3/27/2013	7:00 PM	3/27/2013	7:00 PM	1	0	
Alert processed after gap	3/27/2013	8:00 PM				1	1
Alert Gap	3/28/2013	1:00 AM	3/28/2013	1:00 AM	1	0	
Alert processed after gap	3/28/2013	2:15 AM				4	4
Alert Gap	3/28/2013	5:00 AM	3/28/2013	5:00 AM	1	0	
Alert processed after gap	3/28/2013	6:00 AM				2	2
Alert Gap	3/28/2013	7:00 PM	3/29/2013	5:00 AM	11	0	
Alert processed after gap	3/29/2013	6:00 AM				7	7
Alert Gap	3/29/2013	6:00 PM	4/1/2013	7:00 AM	62	0	
Alert processed after gap	4/1/2013	8:00 AM				377	356
Alert Gap	4/2/2013	12:00 AM	4/2/2013	12:00 AM	1	0	
Alert processed after gap	4/2/2013	1:00 AM				3	3
Alert Gap	4/2/2013	2:00 AM	4/2/2013	2:00 AM	1	0	
Alert processed after gap	4/2/2013	3:00 AM				10	10
Alert Gap	4/2/2013	4:00 AM	4/2/2013	5:00 AM	2	0	
Alert processed after gap	4/2/2013	6:00 AM				1	1
Alert Gap	4/2/2013	7:00 PM	4/2/2013	7:00 PM	1	0	
Alert processed after gap	4/2/2013	8:00 PM				3	3
Alert Gap	4/3/2013	3:00 AM	4/3/2013	5:00 AM	3	0	
Alert processed after gap	4/3/2013	6:00 AM				1	1
Alert Gap	4/3/2013	5:00 PM	4/3/2013	5:00 PM	1	0	
Alert processed after gap	4/3/2013	6:15 PM				17	17
Alert Gap	4/3/2013	7:00 PM	4/4/2013	5:00 AM	11	0	
Alert processed after gap	4/4/2013	6:00 AM				10	10
Alert Gap	4/4/2013	11:00 AM	4/4/2013	11:00 AM	1	0	
Alert processed after gap	4/4/2013	12:00 PM				1	1
Alert Gap	4/4/2013	8:00 PM	4/5/2013	5:00 AM	10	0	

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

Alert processed after gap	4/5/2013	6:00 AM			11	11
Alert Gap	4/5/2013	6:00 PM	4/8/2013	7:00 AM	62	0
Alert processed after gap	4/8/2013	8:00 AM			467	450
Alert Gap	4/8/2013	7:00 PM	4/8/2013	7:00 PM	1	0
Alert processed after gap	4/8/2013	8:00 PM			2	2
Alert Gap	4/9/2013	2:00 AM	4/9/2013	2:00 AM	1	0
Alert processed after gap	4/9/2013	3:15 AM			8	8
Alert Gap	4/9/2013	5:00 AM	4/9/2013	5:00 AM	1	0
Alert processed after gap	4/9/2013	6:15 AM			1	1
Alert Gap	4/9/2013	4:00 PM	4/9/2013	4:00 PM	1	0
Alert processed after gap	4/9/2013	5:30 PM			1	1
Alert Gap	4/9/2013	7:00 PM	4/9/2013	7:00 PM	1	0
Alert processed after gap	4/9/2013	8:00 PM			1	1
Alert Gap	4/10/2013	12:00 AM	4/10/2013	1:00 AM	2	0
Alert processed after gap	4/10/2013	2:30 AM			1	1
Alert Gap	4/10/2013	4:00 AM	4/10/2013	5:00 AM	2	0
Alert processed after gap	4/10/2013	6:00 AM			1	1
Alert Gap	4/10/2013	7:00 PM	4/10/2013	8:00 PM	2	0
Alert processed after gap	4/10/2013	9:00 PM			2	2
Alert Gap	4/11/2013	2:00 AM	4/11/2013	2:00 AM	1	0
Alert processed after gap	4/11/2013	3:30 AM			5	5
Alert Gap	4/11/2013	4:00 AM	4/11/2013	6:00 AM	3	0
Alert processed after gap	4/11/2013	7:00 AM			16	16
Alert Gap	4/11/2013	5:00 PM	4/11/2013	5:00 PM	1	0
Alert processed after gap	4/11/2013	6:00 PM			3	3
Alert Gap	4/11/2013	7:00 PM	4/11/2013	7:00 PM	1	0
Alert processed after gap	4/11/2013	8:00 PM			2	2
Alert Gap	4/11/2013	9:00 PM	4/12/2013	5:00 AM	9	0
Alert processed after gap	4/12/2013	6:00 AM			136	136
Alert Gap	4/12/2013	6:00 PM	4/15/2013	7:00 AM	62	0
Alert processed after gap	4/15/2013	8:00 AM			226	216

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

Alert Gap	4/15/2013	7:00 PM	4/15/2013	7:00 PM	1	0	
Alert processed after gap	4/15/2013	8:00 PM				1	1
Alert Gap	4/16/2013	2:00 AM	4/16/2013	2:00 AM	1	0	
Alert processed after gap	4/16/2013	3:30 AM				10	10
Alert Gap	4/16/2013	4:00 AM	4/16/2013	5:00 AM	2	0	
Alert processed after gap	4/16/2013	6:00 AM				1	1
Alert Gap	4/16/2013	5:00 PM	4/16/2013	5:00 PM	1	0	
Alert processed after gap	4/16/2013	6:15 PM				23	23
Alert Gap	4/16/2013	7:00 PM	4/16/2013	7:00 PM	1	0	
Alert processed after gap	4/16/2013	8:00 PM				2	2
Alert Gap	4/16/2013	9:00 PM	4/17/2013	5:00 AM	9	0	
Alert processed after gap	4/17/2013	6:00 AM				98	98
Alert Gap	4/17/2013	7:00 PM	4/17/2013	7:00 PM	1	0	
Alert processed after gap	4/17/2013	8:00 PM				3	3
Alert Gap	4/18/2013	2:00 AM	4/18/2013	2:00 AM	1	0	
Alert processed after gap	4/18/2013	3:30 AM				7	7
Alert Gap	4/18/2013	4:00 AM	4/18/2013	4:00 AM	1	0	
Alert processed after gap	4/18/2013	5:00 AM				2	2
Alert Gap	4/18/2013	3:00 PM	4/18/2013	3:00 PM	1	0	
Alert processed after gap	4/18/2013	4:00 PM				1	1
Alert Gap	4/18/2013	8:00 PM	4/19/2013	5:00 AM	10	0	
Alert processed after gap	4/19/2013	6:00 AM				216	216
Alert Gap	4/19/2013	7:00 AM	4/19/2013	7:00 AM	1	0	
Alert processed after gap	4/19/2013	8:15 AM				1	1
Alert Gap	4/19/2013	6:00 PM	4/22/2013	7:00 AM	62	0	
Alert processed after gap	4/22/2013	8:00 AM				96	94
Alert Gap	4/22/2013	4:00 PM	4/22/2013	5:00 PM	2	0	
Alert processed after gap	4/22/2013	6:15 PM				22	22
Alert Gap	4/22/2013	7:00 PM	4/22/2013	7:00 PM	1	0	
Alert processed after gap	4/22/2013	8:00 PM				1	1
Alert Gap	4/23/2013	2:00 AM	4/23/2013	2:00 AM	1	0	

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

Alert processed after gap	4/23/2013	3:30 AM			4	4
Alert Gap	4/23/2013	4:00 AM	4/23/2013	5:00 AM	2	0
Alert processed after gap	4/23/2013	6:00 AM			1	1
Alert Gap	4/23/2013	1:00 PM	4/23/2013	1:00 PM	1	0
Alert processed after gap	4/23/2013	2:15 PM			1	1
Alert Gap	4/23/2013	7:00 PM	4/23/2013	7:00 PM	1	0
Alert processed after gap	4/23/2013	8:00 PM			1	1
Alert Gap	4/24/2013	2:00 AM	4/24/2013	2:00 AM	1	0
Alert processed after gap	4/24/2013	3:30 AM			4	4
Alert Gap	4/24/2013	4:00 AM	4/24/2013	6:00 AM	3	0
Alert processed after gap	4/24/2013	7:30 AM			1	1
Alert Gap	4/24/2013	5:00 PM	4/24/2013	5:00 PM	1	0
Alert processed after gap	4/24/2013	6:15 PM			9	9
Alert Gap	4/24/2013	8:00 PM	4/24/2013	8:00 PM	1	0
Alert processed after gap	4/24/2013	9:00 PM			22	22
Alert Gap	4/25/2013	4:00 AM	4/25/2013	4:00 AM	1	0
Alert processed after gap	4/25/2013	5:15 AM			3	3
Alert Gap	4/25/2013	7:00 PM	4/25/2013	7:00 PM	1	0
Alert processed after gap	4/25/2013	8:00 PM			2	2
Alert Gap	4/25/2013	9:00 PM	4/26/2013	5:00 AM	9	0
Alert processed after gap	4/26/2013	6:15 AM			238	235
Alert Gap	4/26/2013	5:00 PM	4/29/2013	7:00 AM	63	0
Alert processed after gap	4/29/2013	8:00 AM			427	410
Alert Gap	4/29/2013	4:00 PM	4/29/2013	5:00 PM	2	0
Alert processed after gap	4/29/2013	6:00 PM			1	1
Alert Gap	4/30/2013	2:00 AM	4/30/2013	2:00 AM	1	0
Alert processed after gap	4/30/2013	3:45 AM			4	4
Alert Gap	4/30/2013	4:00 AM	4/30/2013	4:00 AM	1	0
Alert processed after gap	4/30/2013	5:00 AM			1	1
Alert Gap	4/30/2013	6:00 AM	4/30/2013	6:00 AM	1	0
Alert processed after gap	4/30/2013	7:00 AM			2	2

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

Alert Gap	4/30/2013	5:00 PM	4/30/2013	5:00 PM	1	0
Alert processed after gap	4/30/2013	6:15 PM				14
Alert Gap	4/30/2013	7:00 PM	4/30/2013	7:00 PM	1	0
Alert processed after gap	4/30/2013	8:00 PM				3
Alert Gap	4/30/2013	9:00 PM	5/1/2013	12:00 PM	16	0
Alert processed after gap	5/1/2013	1:00 PM				298
Alert Gap	5/1/2013	7:00 PM	5/1/2013	7:00 PM	1	0
Alert processed after gap	5/1/2013	8:00 PM				1
Alert Gap	5/2/2013	1:00 AM	5/2/2013	1:00 AM	1	0
Alert processed after gap	5/2/2013	2:15 AM				3
Alert Gap	5/2/2013	3:00 AM	5/2/2013	4:00 AM	2	0
Alert processed after gap	5/2/2013	5:15 AM				6
Alert Gap	5/2/2013	5:00 PM	5/2/2013	6:00 PM	2	0
Alert processed after gap	5/2/2013	7:00 PM				1
Alert Gap	5/2/2013	8:00 PM	5/2/2013	8:00 PM	1	0
Alert processed after gap	5/2/2013	9:00 PM				1
Alert Gap	5/3/2013	2:00 AM	5/3/2013	2:00 AM	1	0
Alert processed after gap	5/3/2013	3:30 AM				4
Alert Gap	5/3/2013	4:00 AM	5/3/2013	5:00 AM	2	0
Alert processed after gap	5/3/2013	6:00 AM				4
Alert Gap	5/3/2013	6:00 PM	5/6/2013	7:00 AM	62	0
Alert processed after gap	5/6/2013	8:00 AM				365
Alert Gap	5/6/2013	3:00 PM	5/6/2013	3:00 PM	1	0
Alert processed after gap	5/6/2013	4:00 PM				1
Alert Gap	5/6/2013	5:00 PM	5/6/2013	5:00 PM	1	0
Alert processed after gap	5/6/2013	6:15 PM				28
Alert Gap	5/6/2013	7:00 PM	5/6/2013	7:00 PM	1	0
Alert processed after gap	5/6/2013	8:00 PM	5/6/2013			1
Alert Gap	5/7/2013	9:00 PM	5/8/2013	4:00 AM	8	0
Alert processed after gap	5/8/2013	5:45 AM				277
Alert Gap	5/8/2013	7:00 PM	5/8/2013	7:00 PM	1	0

(b)(3);6(f);(b)(4)

Alert processed after gap	5/8/2013	8:00 PM			1	1
Alert Gap	5/9/2013	1:00 AM	5/9/2013	3:00 AM	3	0
Alert processed after gap	5/9/2013	4:00 AM			4	4
Alert Gap	5/9/2013	2:00 PM	5/9/2013	3:00 PM	2	0
Alert processed after gap	5/9/2013	4:00 PM			16	16
Alert Gap	5/9/2013	7:00 PM	5/9/2013	8:00 PM	2	0
Alert processed after gap	5/9/2013	9:00 PM			2	2
Alert Gap	5/10/2013	2:00 AM	5/10/2013	2:00 AM	1	0
Alert processed after gap	5/10/2013	3:00 AM			2	2
Alert Gap	5/10/2013	6:00 PM	5/13/2013	7:00 AM	62	0
Alert processed after gap	5/13/2013	8:00 AM			423	403
Alert Gap	5/13/2013	2:00 PM	5/13/2013	3:00 PM	2	0
Alert processed after gap	5/13/2013	4:00 PM			54	53
Alert Gap	5/13/2013	7:00 PM	5/13/2013	7:00 PM	1	0
Alert processed after gap	5/13/2013	8:00 PM			1	1
Alert Gap	5/14/2013	2:00 AM	5/14/2013	4:00 AM	3	0
Alert processed after gap	5/14/2013	5:15 AM			3	3
Alert Gap	5/14/2013	7:00 PM	5/14/2013	7:00 PM	1	0
Alert processed after gap	5/14/2013	8:00 PM			1	1
Alert Gap	5/14/2013	9:00 PM	5/15/2013	5:00 AM	9	0
Alert processed after gap	5/15/2013	6:15 AM			244	244
Alert Gap	5/15/2013	7:00 PM	5/16/2013	5:00 AM	11	0
Alert processed after gap	5/16/2013	6:15 AM			266	266
Alert Gap	5/16/2013	6:00 PM	5/16/2013	7:00 PM	2	0
Alert processed after gap	5/16/2013	8:00 PM			15	15
Alert Gap	5/17/2013	2:00 AM	5/17/2013	2:00 AM	1	0
Alert processed after gap	5/17/2013	3:15 AM			1	1
Alert Gap	5/17/2013	5:00 AM	5/17/2013	5:00 AM	1	0
Alert processed after gap	5/17/2013	6:30 AM			1	1
Alert Gap	5/17/2013	6:00 PM	5/20/2013	7:00 AM	62	0
Alert processed after gap	5/20/2013	8:00 AM			326	292

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

Alert Gap	5/20/2013	7:00 PM	5/20/2013	7:00 PM	1	0
Alert processed after gap	5/20/2013	8:00 PM				2
Alert Gap	5/21/2013	12:00 AM	5/21/2013	12:00 AM	1	0
Alert processed after gap	5/21/2013	1:15 AM				4
Alert Gap	5/21/2013	5:00 AM	5/21/2013	5:00 AM	1	0
Alert processed after gap	5/21/2013	6:00 AM				2
Alert Gap	5/21/2013	12:00 PM	5/21/2013	12:00 PM	1	0
Alert processed after gap	5/21/2013	1:00 PM				8
Alert Gap	5/21/2013	9:00 PM	5/22/2013	6:00 AM	10	0
Alert processed after gap	5/22/2013	7:00 AM				157
Alert Gap	5/22/2013	7:00 PM	5/22/2013	7:00 PM	1	0
Alert processed after gap	5/22/2013	8:00 PM				2
Alert Gap	5/23/2013	2:00 AM	5/23/2013	2:00 AM	1	0
Alert processed after gap	5/23/2013	3:30 AM				1
Alert Gap	5/23/2013	7:00 PM	5/24/2013	5:00 AM	11	0
Alert processed after gap	5/24/2013	6:15 AM				93
Alert Gap	5/24/2013	7:00 AM	5/24/2013	7:00 AM	1	0
Alert processed after gap	5/24/2013	8:45 AM				15
Alert Gap	5/24/2013	6:00 PM	5/28/2013	7:00 AM	86	0
Alert processed after gap	5/28/2013	8:00 AM				383
Alert Gap	5/28/2013	12:00 PM	5/28/2013	12:00 PM	1	0
Alert processed after gap	5/28/2013	1:00 PM				2
Alert Gap	5/28/2013	7:00 PM	5/28/2013	7:00 PM	1	0
Alert processed after gap	5/28/2013	8:00 PM				4
Alert Gap	5/29/2013	2:00 AM	5/29/2013	2:00 AM	1	0
Alert processed after gap	5/29/2013	3:00 AM				18
Alert Gap	5/29/2013	5:00 AM	5/29/2013	5:00 AM	1	0
Alert processed after gap	5/29/2013	6:15 AM				2
Alert Gap	5/29/2013	7:00 PM	5/29/2013	7:00 PM	1	0
Alert processed after gap	5/29/2013	8:00 PM				1
Alert Gap	5/30/2013	6:00 AM	5/30/2013	6:00 AM	1	0

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

Alert processed after gap	5/30/2013	7:00 AM			1	1
Alert Gap	5/30/2013	8:00 PM	5/31/2013	5:00 AM	10	0
Alert processed after gap	5/31/2013	6:00 AM			2	2
Alert Gap	5/31/2013	6:00 PM	6/3/2013	7:00 AM	62	0
Alert processed after gap	6/3/2013	8:00 AM			341	314
Alert Gap	6/3/2013	7:00 PM	6/3/2013	7:00 PM	1	0
Alert processed after gap	6/3/2013	8:00 PM			2	2
Alert Gap	6/4/2013	8:00 PM	6/4/2013	9:00 PM	2	0
Alert processed after gap	6/4/2013	10:15 PM			79	79
Alert Gap	6/5/2013	3:00 AM	6/5/2013	3:00 AM	1	0
Alert processed after gap	6/5/2013	4:15 AM			5	5
Alert Gap	6/5/2013	5:00 AM	6/5/2013	5:00 AM	1	0
Alert processed after gap	6/5/2013	6:15 AM			1	1
Alert Gap	6/5/2013	7:00 PM	6/5/2013	7:00 PM	1	0
Alert processed after gap	6/5/2013	8:00 PM			1	1
Alert Gap	6/5/2013	9:00 PM	6/6/2013	5:00 AM	9	0
Alert processed after gap	6/6/2013	6:00 AM			301	300
Alert Gap	6/6/2013	9:00 AM	6/6/2013	9:00 AM	1	0
Alert processed after gap	6/6/2013	10:15 AM			2	2
Alert Gap	6/6/2013	7:00 PM	6/6/2013	7:00 PM	1	0
Alert processed after gap	6/6/2013	8:00 PM			3	3
Alert Gap	6/7/2013	2:00 AM	6/7/2013	2:00 AM	1	0
Alert processed after gap	6/7/2013	3:15 AM			5	5
Alert Gap	6/7/2013	6:00 PM	6/10/2013	7:00 AM	62	0
Alert processed after gap	6/10/2013	8:00 AM			252	216
Alert Gap	6/10/2013	7:00 PM	6/10/2013	7:00 PM	1	0
Alert processed after gap	6/10/2013	8:00 PM			3	3
Alert Gap	6/10/2013	9:00 PM	6/10/2013	9:00 PM	1	0
Alert processed after gap	6/10/2013	10:00 PM			17	17
Alert Gap	6/11/2013	7:00 PM	6/12/2013	5:00 AM	11	0
Alert processed after gap	6/12/2013	6:00 AM			93	93

(b)(3);6(f);(b)(4)

Alert Gap	6/12/2013	7:00 PM	6/12/2013	7:00 PM	1	0	
Alert processed after gap	6/12/2013	8:00 PM				1	1
Alert Gap	6/13/2013	2:00 AM	6/13/2013	2:00 AM	1	0	
Alert processed after gap	6/13/2013	3:30 AM				6	6
Alert Gap	6/13/2013	4:00 AM	6/13/2013	5:00 AM	2	0	
Alert processed after gap	6/13/2013	6:15 AM				1	1
Alert Gap	6/13/2013	5:00 PM	6/13/2013	5:00 PM	1	0	
Alert processed after gap	6/13/2013	6:00 PM				1	1
Alert Gap	6/13/2013	7:00 PM	6/14/2013	5:00 AM	11	0	
Alert processed after gap	6/14/2013	6:00 AM				254	254
Alert Gap	6/14/2013	6:00 PM	6/17/2013	7:00 AM	62	0	
Alert processed after gap	6/17/2013	8:30 AM				22	22
Alert Gap	6/17/2013	8:00 PM	6/17/2013	8:00 PM	1	0	
Alert processed after gap	6/17/2013	9:00 PM				1	1
Alert Gap	6/18/2013	2:00 AM	6/18/2013	3:00 AM	2	0	
Alert processed after gap	6/18/2013	4:30 AM				2	2
Alert Gap	6/18/2013	7:00 PM	6/18/2013	7:00 PM	1	0	
Alert processed after gap	6/18/2013	8:15 PM				1	1
Alert Gap	6/18/2013	9:00 PM	6/19/2013	5:00 AM	9	0	
Alert processed after gap	6/19/2013	6:15 AM				159	159
Alert Gap	6/19/2013	5:00 PM	6/19/2013	5:00 PM	1	0	
Alert processed after gap	6/19/2013	6:15 PM				13	13
Alert Gap	6/19/2013	7:00 PM	6/19/2013	7:00 PM	1	0	
Alert processed after gap	6/19/2013	8:00 PM				1	1
Alert Gap	6/20/2013	2:00 AM	6/20/2013	2:00 AM	1	0	
Alert processed after gap	6/20/2013	3:30 AM				3	3
Alert Gap	6/20/2013	4:00 AM	6/20/2013	4:00 AM	1	0	
Alert processed after gap	6/20/2013	5:00 AM				3	3
Alert Gap	6/20/2013	6:00 AM	6/20/2013	6:00 AM	1	0	
Alert processed after gap	6/20/2013	7:15 AM				1	1
Alert Gap	6/20/2013	8:00 AM	6/20/2013	8:00 AM	1	0	

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

Alert processed after gap	6/20/2013	9:00 AM			4	4
Alert Gap	6/20/2013	7:00 PM	6/20/2013	7:00 PM	1	0
Alert processed after gap	6/20/2013	8:00 PM			3	3
Alert Gap	6/20/2013	10:00 PM	6/21/2013	5:00 AM	8	0
Alert processed after gap	6/21/2013	6:15 AM			29	29
Alert Gap	6/21/2013	5:00 PM	6/24/2013	7:00 AM	63	0
Alert processed after gap	6/24/2013	8:00 AM			340	328
Alert Gap	6/24/2013	7:00 PM	6/24/2013	9:00 PM	3	0
Alert processed after gap	6/24/2013	10:00 PM			17	17
Alert Gap	6/25/2013	2:00 AM	6/25/2013	2:00 AM	1	0
Alert processed after gap	6/25/2013	3:45 AM			6	6
Alert Gap	6/25/2013	7:00 PM	6/26/2013	5:00 AM	11	0
Alert processed after gap	6/26/2013	6:00 AM			93	93
Alert Gap	6/26/2013	7:00 PM	6/26/2013	7:00 PM	1	0
Alert processed after gap	6/26/2013	8:00 PM			3	3
Alert Gap	6/27/2013	2:00 AM	6/27/2013	2:00 AM	1	0
Alert processed after gap	6/27/2013	3:15 AM			1	1
Alert Gap	6/27/2013	8:00 AM	6/27/2013	8:00 AM	1	0
Alert processed after gap	6/27/2013	9:00 AM			8	8
Alert Gap	6/27/2013	5:00 PM	7/1/2013	8:00 AM	88	0
Alert processed after gap	7/1/2013	9:30 AM			31	29
Alert Gap	7/1/2013	7:00 PM	7/1/2013	7:00 PM	1	0
Alert processed after gap	7/1/2013	8:00 PM			2	2
Alert Gap	7/2/2013	4:00 AM	7/2/2013	4:00 AM	1	0
Alert processed after gap	7/2/2013	5:15 AM			4	4
Alert Gap	7/2/2013	7:00 PM	7/2/2013	8:00 PM	2	0
Alert processed after gap	7/2/2013	9:00 PM			2	2
Alert Gap	7/3/2013	2:00 AM	7/3/2013	2:00 AM	1	0
Alert processed after gap	7/3/2013	3:15 AM			2	2
Alert Gap	7/3/2013	5:00 AM	7/3/2013	5:00 AM	1	0

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

Alert processed after gap	7/3/2013	6:00 AM			1	1
Alert Gap	7/3/2013	7:00 PM	7/3/2013	8:00 PM	2	0
Alert processed after gap	7/3/2013	9:00 PM			3	3
Alert Gap	7/4/2013	2:00 AM	7/4/2013	2:00 AM	1	0
Alert processed after gap	7/4/2013	3:30 AM			7	7
Alert Gap	7/4/2013	7:00 AM	7/4/2013	8:00 AM	2	0
Alert processed after gap	7/4/2013	9:00 AM			1	1
Alert Gap	7/4/2013	11:00 AM	7/4/2013	12:00 PM	2	0
Alert processed after gap	7/4/2013	1:15 PM			1	1
Alert Gap	7/4/2013	2:00 PM	7/4/2013	8:00 PM	7	0
Alert processed after gap	7/4/2013	9:45 PM			1	1
Alert Gap	7/4/2013	10:00 PM	7/4/2013	10:00 PM	1	0
Alert processed after gap	7/4/2013	11:00 PM			49	49
Alert Gap	7/5/2013	12:00 AM	7/5/2013	6:00 AM	7	0
Alert processed after gap	7/5/2013	7:00 AM			2	2
Alert Gap	7/5/2013	5:00 PM	7/8/2013	6:00 AM	63	0
Alert processed after gap	7/8/2013	8:00 AM			285	269
Alert Gap	7/8/2013	7:00 PM	7/8/2013	7:00 PM	1	0
Alert processed after gap	7/8/2013	8:00 PM			2	2
Alert Gap	7/8/2013	9:00 PM	7/8/2013	9:00 PM	1	0
Alert processed after gap	7/8/2013	10:15 PM			101	101
Alert Gap	7/9/2013	2:00 AM	7/9/2013	2:00 AM	1	0
Alert processed after gap	7/9/2013	3:30 AM			9	9
Alert Gap	7/9/2013	7:00 PM	7/9/2013	7:00 PM	1	0
Alert processed after gap	7/9/2013	8:00 PM			2	2
Alert Gap	7/10/2013	2:00 AM	7/10/2013	2:00 AM	1	0
Alert processed after gap	7/10/2013	3:45 AM			1	1
Alert Gap	7/10/2013	5:00 PM	7/10/2013	5:00 PM	1	0
Alert processed after gap	7/10/2013	6:15 PM			22	22
Alert Gap	7/10/2013	7:00 PM	7/10/2013	7:00 PM	1	0
Alert processed after gap	7/10/2013	8:15 PM			1	1

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

Alert Gap	7/11/2013	2:00 AM	7/11/2013	2:00 AM	1	0
Alert processed after gap	7/11/2013	3:45 AM				5
Alert Gap	7/11/2013	4:00 AM	7/11/2013	5:00 AM	2	0
Alert processed after gap	7/11/2013	6:00 AM				1
Alert Gap	7/11/2013	5:00 PM	7/11/2013	5:00 PM	1	0
Alert processed after gap	7/11/2013	6:15 PM				18
Alert Gap	7/11/2013	7:00 PM	7/11/2013	7:00 PM	1	0
Alert processed after gap	7/11/2013	8:00 PM				2
Alert Gap	7/12/2013	2:00 AM	7/12/2013	2:00 AM	1	0
Alert processed after gap	7/12/2013	3:15 AM				2
Alert Gap	7/12/2013	4:00 AM	7/12/2013	4:00 AM	1	0
Alert processed after gap	7/12/2013	5:30 AM				3
Alert Gap	7/12/2013	6:00 PM	7/12/2013	7:00 PM	2	0
Alert processed after gap	7/12/2013	8:15 PM	7/12/2013	8:15 PM		2
Alert Gap	7/13/2013	2:00 PM	7/13/2013	2:00 PM	1	0
Alert processed after gap	7/13/2013	3:00 PM				1
Alert Gap	7/13/2013	7:00 PM	7/13/2013	7:00 PM	1	0
Alert processed after gap	7/13/2013	8:00 PM				2
Alert Gap	7/13/2013	9:00 PM	7/14/2013	12:00 AM	4	0
Alert processed after gap	7/14/2013	1:00 AM				38
Alert Gap	7/14/2013	9:00 AM	7/14/2013	9:00 AM	1	0
Alert processed after gap	7/14/2013	10:30 AM				1
Alert Gap	7/14/2013	11:00 AM	7/14/2013	5:00 PM	7	0
Alert processed after gap	7/14/2013	8:30 PM				135
Alert Gap	7/14/2013	9:00 PM	7/15/2013	4:00 AM	10	0
Alert processed after gap	7/15/2013	5:45 AM				1
Alert Gap	7/15/2013	7:00 PM	7/15/2013	7:00 PM	1	0
Alert processed after gap	7/15/2013	8:15 PM				1
Alert Gap	7/16/2013	5:00 AM	7/16/2013	5:00 AM	1	0
Alert processed after gap	7/16/2013	6:00 AM				1
Alert Gap	7/16/2013	5:00 PM	7/16/2013	5:00 PM	1	0

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

Alert processed after gap	7/16/2013	6:15 PM				17	17
Alert Gap	7/16/2013	7:00 PM	7/16/2013	7:00 PM	1	0	
Alert processed after gap	7/16/2013	8:15 PM				1	1
Alert Gap	7/17/2013	2:00 AM	7/17/2013	2:00 AM	1	0	
Alert processed after gap	7/17/2013	3:30 AM				8	7
Alert Gap	7/17/2013	6:00 AM	7/17/2013	6:00 AM	1	0	
Alert processed after gap	7/17/2013	7:00 AM				2	2
Alert Gap	7/17/2013	7:00 PM	7/17/2013	7:00 PM	1	0	
Alert processed after gap	7/17/2013	8:15 PM				2	2
Alert Gap	7/18/2013	1:00 AM	7/18/2013	2:00 AM	2	0	
Alert processed after gap	7/18/2013	3:45 AM				6	6
Alert Gap	7/18/2013	7:00 PM	7/18/2013	7:00 PM	1	0	
Alert processed after gap	7/18/2013	8:00 PM				1	1
Alert Gap	7/19/2013	2:00 AM	7/19/2013	2:00 AM	1	0	
Alert processed after gap	7/19/2013	3:15 AM				2	2
Alert Gap	7/19/2013	4:00 AM	7/19/2013	4:00 AM	1	0	
Alert processed after gap	7/19/2013	5:15 AM				1	1
Alert Gap	7/19/2013	6:00 PM	7/23/2013	7:00 AM	86	0	
Alert processed after gap	7/23/2013	8:00 AM				558	499
Alert Gap	7/23/2013	9:00 AM	7/23/2013	9:00 AM	1	0	
Alert processed after gap	7/23/2013	10:30 AM				473	419
Alert Gap	7/23/2013	7:00 PM	7/23/2013	8:00 PM	2	0	
Alert processed after gap	7/23/2013	9:00 PM				1	1
Alert Gap	7/24/2013	2:00 AM	7/24/2013	2:00 AM	1	0	
Alert processed after gap	7/24/2013	3:30 AM				9	9
Alert Gap	7/24/2013	5:00 AM	7/24/2013	5:00 AM	1	0	
Alert processed after gap	7/24/2013	6:00 AM				1	1
Alert Gap	7/24/2013	7:00 PM	7/24/2013	7:00 PM	1	0	
Alert processed after gap	7/24/2013	8:00 PM				5	5
Alert Gap	7/25/2013	2:00 AM	7/25/2013	2:00 AM	1	0	
Alert processed after gap	7/25/2013	3:30 AM				4	4

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

Alert Gap	7/25/2013	4:00 AM	7/25/2013	4:00 AM	1	0
Alert processed after gap	7/25/2013	5:15 AM				2
Alert Gap	7/25/2013	7:00 PM	7/25/2013	7:00 PM	1	0
Alert processed after gap	7/25/2013	8:00 PM				3
Alert Gap	7/26/2013	1:00 AM	7/26/2013	2:00 AM	2	0
Alert processed after gap	7/26/2013	3:30 AM				11
Alert Gap	7/26/2013	4:00 AM	7/26/2013	1:00 PM	10	0
Alert processed after gap	7/26/2013	2:15 PM				42
Alert Gap	7/27/2013	11:00 AM	7/27/2013	11:00 AM	1	0
Alert processed after gap	7/27/2013	12:15 PM				19
Alert Gap	7/27/2013	2:00 PM	7/27/2013	2:00 PM	1	0
Alert processed after gap	7/27/2013	3:15 PM				1
Alert Gap	7/27/2013	7:00 PM	7/27/2013	7:00 PM	1	0
Alert processed after gap	7/27/2013	8:00 PM				1
Alert Gap	7/27/2013	9:00 PM	7/27/2013	11:00 PM	3	0
Alert processed after gap	7/28/2013	12:00 AM				108
Alert Gap	7/28/2013	7:00 AM	7/28/2013	4:00 PM	10	0
Alert processed after gap	7/28/2013	5:30 PM				73
Alert Gap	7/28/2013	6:00 PM	7/28/2013	8:00 PM	3	0
Alert processed after gap	7/28/2013	9:45 PM				1
Alert Gap	7/28/2013	10:00 PM	7/28/2013	11:00 PM	2	0
Alert processed after gap	7/29/2013	12:15 AM				1
Alert Gap	7/29/2013	1:00 AM	7/29/2013	4:00 AM	4	0
Alert processed after gap	7/29/2013	5:45 AM				1
Alert Gap	7/29/2013	8:00 AM	7/29/2013	8:00 AM	1	0
Alert processed after gap	7/29/2013	9:00 AM				4
Alert Gap	7/29/2013	7:00 PM	7/29/2013	7:00 PM	1	0
Alert processed after gap	7/29/2013	8:00 PM				1
Alert Gap	7/29/2013	9:00 PM	7/30/2013	4:00 AM	8	0
Alert processed after gap	7/30/2013	5:45 AM				44
Alert Gap	7/30/2013	5:00 PM	7/30/2013	10:00 PM	6	0

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

Alert processed after gap	7/30/2013	11:00 PM				172	168
Alert Gap	7/31/2013	1:00 AM	7/31/2013	1:00 AM	1	0	
Alert processed after gap	7/31/2013	2:15 AM				1	1
Alert Gap	7/31/2013	4:00 AM	7/31/2013	4:00 AM	1	0	
Alert processed after gap	7/31/2013	5:15 AM				2	2
Alert Gap	8/1/2013	2:00 AM	8/1/2013	3:00 AM	2	0	
Alert processed after gap	8/1/2013	4:00 AM				5	5
Alert Gap	8/1/2013	7:00 PM	8/1/2013	8:00 PM	2	0	
Alert processed after gap	8/1/2013	9:00 PM				14	14
Alert Gap	8/2/2013	4:00 AM	8/2/2013	5:00 AM	2	0	
Alert processed after gap	8/2/2013	6:00 AM				2	2
Alert Gap	8/2/2013	7:00 PM	8/5/2013	9:00 AM	63	0	
Alert processed after gap	8/5/2013	10:45 AM				308	306
Alert Gap	8/6/2013	5:00 AM	8/6/2013	5:00 AM	1	0	
Alert processed after gap	8/6/2013	6:00 AM				1	1
Alert Gap	8/6/2013	7:00 PM	8/6/2013	7:00 PM	1	0	
Alert processed after gap	8/6/2013	8:00 PM				1	1
Alert Gap	8/7/2013	2:00 AM	8/7/2013	2:00 AM	1	0	
Alert processed after gap	8/7/2013	3:30 AM				13	13
Alert Gap	8/7/2013	4:00 AM	8/7/2013	4:00 AM	1	0	
Alert processed after gap	8/7/2013	5:45 AM				1	1
Alert Gap	8/7/2013	7:00 PM	8/7/2013	8:00 PM	2	0	
Alert processed after gap	8/7/2013	9:00 PM				20	20
Alert Gap	8/8/2013	2:00 AM	8/8/2013	2:00 AM	1	0	
Alert processed after gap	8/8/2013	3:30 AM				4	4
Alert Gap	8/8/2013	5:00 AM	8/8/2013	5:00 AM	1	0	
Alert processed after gap	8/8/2013	6:00 AM				3	3
Alert Gap	8/8/2013	7:00 PM	8/8/2013	7:00 PM	1	0	
Alert processed after gap	8/8/2013	8:15 PM				2	2
Alert Gap	8/9/2013	2:00 AM	8/9/2013	2:00 AM	1	0	
Alert processed after gap	8/9/2013	3:30 AM				11	10

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

Alert Gap	8/9/2013	4:00 AM	8/9/2013	5:00 AM	2	0	(b)(3);6(f),(b)(4)	
Alert processed after gap	8/9/2013	6:30 AM				3		3
Alert Gap	8/9/2013	7:00 PM	8/9/2013	7:00 PM	1	0		
Alert processed after gap	8/9/2013	8:15 PM				2		2
Alert Gap	8/10/2013	2:00 AM	8/10/2013	2:00 AM	1	0		
Alert processed after gap	8/10/2013	3:30 AM				7		7
Alert Gap	8/10/2013	1:00 PM	8/10/2013	1:00 PM	1	0		
Alert processed after gap	8/10/2013	2:15 PM				1		1
Alert Gap	8/11/2013	7:00 AM	8/11/2013	8:00 PM	14	0		
Alert processed after gap	8/11/2013	9:00 PM				57		53
Alert Gap	8/11/2013	10:00 PM	8/12/2013	5:00 AM	8	0		
Alert processed after gap	8/12/2013	6:00 AM				4		4
Alert Gap	8/12/2013	4:00 PM	8/12/2013	5:00 PM	2	0		
Alert processed after gap	8/12/2013	6:00 PM				1		1
Alert Gap	8/12/2013	7:00 PM	8/12/2013	7:00 PM	1	0		
Alert processed after gap	8/12/2013	8:30 PM				1		1
Alert Gap	8/13/2013	5:00 AM	8/13/2013	5:00 AM	1	0		
Alert processed after gap	8/13/2013	6:00 AM				2		2
Alert Gap	8/13/2013	5:00 PM	8/13/2013	5:00 PM	1	0		
Alert processed after gap	8/13/2013	6:15 PM				20		20
Alert Gap	8/13/2013	7:00 PM	8/13/2013	8:00 PM	2	0		
Alert processed after gap	8/13/2013	9:00 PM				1		1
Alert Gap	8/14/2013	2:00 AM	8/14/2013	2:00 AM	1	0		
Alert processed after gap	8/14/2013	3:30 AM				8		8
Alert Gap	8/14/2013	4:00 AM	8/14/2013	4:00 AM	1	0		
Alert processed after gap	8/14/2013	5:45 AM				3		3
Alert Gap	8/14/2013	7:00 PM	8/14/2013	7:00 PM	1	0		
Alert processed after gap	8/14/2013	8:15 PM				1		1
Alert Gap	8/15/2013	1:00 AM	8/15/2013	2:00 AM	2	0		
Alert processed after gap	8/15/2013	3:15 AM				1		1
Alert Gap	8/15/2013	5:00 AM	8/15/2013	5:00 AM	1	0		

Alert processed after gap	8/15/2013	6:45 AM			1	1
Alert Gap	8/15/2013	10:00 PM	8/15/2013	10:00 PM	1	0
Alert processed after gap	8/15/2013	11:00 PM				21
Alert Gap	8/15/2013	1:00 PM	8/15/2013	4:00 PM	4	0
Alert processed after gap	8/16/2013	5:45 AM				59
Alert Gap	8/16/2013	7:00 PM	8/16/2013	8:00 PM	2	0
Alert processed after gap	8/16/2013	9:00 PM				22
Alert Gap	8/17/2013	2:00 AM	8/17/2013	2:00 AM	1	0
Alert processed after gap	8/17/2013	3:30 AM				4
Alert Gap	8/17/2013	6:00 AM	8/17/2013	6:00 AM	1	0
Alert processed after gap	8/17/2013	7:15 AM				1
Alert Gap	8/17/2013	12:00 PM	8/17/2013	12:00 PM	1	0
Alert processed after gap	8/17/2013	1:00 PM				2
Alert Gap	8/18/2013	12:00 PM	8/18/2013	5:00 PM	6	0
Alert processed after gap	8/18/2013	6:15 PM				56
Alert Gap	8/18/2013	7:00 PM	8/19/2013	4:00 AM	10	0
Alert processed after gap	8/19/2013	5:00 AM				1
Alert Gap	8/19/2013	5:00 PM	8/19/2013	5:00 PM	1	0
Alert processed after gap	8/19/2013	6:15 PM				37
Alert Gap	8/20/2013	2:00 AM	8/20/2013	2:00 AM	1	0
Alert processed after gap	8/20/2013	3:45 AM				8
Alert Gap	8/20/2013	7:00 PM	8/20/2013	7:00 PM	1	0
Alert processed after gap	8/20/2013	8:00 PM				1
Alert Gap	8/20/2013	11:00 PM	8/21/2013	2:00 AM	4	0
Alert processed after gap	8/21/2013	3:00 AM				187
Alert Gap	8/21/2013	5:00 PM	8/21/2013	5:00 PM	1	0
Alert processed after gap	8/21/2013	6:15 AM				23
Alert Gap	8/21/2013	7:00 PM	8/21/2013	8:00 PM	2	0
Alert processed after gap	8/21/2013	9:00 PM				1
Alert Gap	8/22/2013	2:00 AM	8/22/2013	2:00 AM	1	0
Alert processed after gap	8/22/2013	3:30 AM				6

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

Alert Gap	8/22/2013	4:00 AM	8/22/2013	4:00 AM	1	0
Alert processed after gap	8/22/2013	5:30 AM				1
Alert Gap	8/22/2013	7:00 PM	8/22/2013	7:00 PM	1	0
Alert processed after gap	8/22/2013	8:00 PM				3
Alert Gap	8/22/2013	9:00 PM	8/23/2013	5:00 AM	9	0
Alert processed after gap	8/23/2013	6:15 AM				282
Alert Gap	8/23/2013	7:00 PM	8/23/2013	8:00 PM	2	0
Alert processed after gap	8/23/2013	9:00 PM				13
Alert Gap	8/24/2013	4:00 AM	8/24/2013	5:00 AM	2	0
Alert processed after gap	8/24/2013	6:00 AM				1
Alert Gap	8/24/2013	2:00 PM	8/24/2013	2:00 PM	1	0
Alert processed after gap	8/24/2013	3:00 PM				2
Alert Gap	8/24/2013	5:00 PM	8/24/2013	8:00 PM	4	0
Alert processed after gap	8/24/2013	9:00 PM				1
Alert Gap	8/24/2013	10:00 PM	8/24/2013	10:00 PM	1	0
Alert processed after gap	8/24/2013	11:00 PM				34
Alert Gap	8/25/2013	4:00 AM	8/25/2013	5:00 AM	2	0
Alert processed after gap	8/25/2013	6:00 AM				87
Alert Gap	8/25/2013	10:00 AM	8/25/2013	4:00 PM	7	0
Alert processed after gap	8/25/2013	5:00 PM				63
Alert Gap	8/25/2013	6:00 PM	8/26/2013	5:00 AM	12	0
Alert processed after gap	8/26/2013	6:00 AM				4
Alert Gap	8/26/2013	3:00 PM	8/26/2013	3:00 PM	1	0
Alert processed after gap	8/26/2013	4:00 PM				2
Alert Gap	8/26/2013	5:00 PM	8/26/2013	5:00 PM	1	0
Alert processed after gap	8/26/2013	6:15 PM				30
Alert Gap	8/26/2013	7:00 PM	8/26/2013	8:00 PM	2	0
Alert processed after gap	8/26/2013	9:00 PM				1
Alert Gap	8/27/2013	2:00 AM	8/27/2013	2:00 AM	1	0
Alert processed after gap	8/27/2013	3:30 AM				15
Alert Gap	8/27/2013	4:00 AM	8/27/2013	4:00 AM	1	0

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

Alert processed after gap	8/27/2013	5:00 AM			2	2
Alert Gap	8/27/2013	3:00 PM	8/27/2013	3:00 PM	1	0
Alert processed after gap	8/27/2013	4:30 PM			2	2
Alert Gap	8/27/2013	7:00 PM	8/27/2013	7:00 PM	1	0
Alert processed after gap	8/27/2013	8:00 PM			3	3
Alert Gap	8/27/2013	9:00 PM	8/28/2013	5:00 AM	9	0
Alert processed after gap	8/28/2013	6:00 AM			211	209
Alert Gap	8/28/2013	7:00 PM	8/28/2013	7:00 PM	1	0
Alert processed after gap	8/28/2013	8:00 PM			4	4
Alert Gap	8/29/2013	5:00 AM	8/29/2013	5:00 AM	1	0
Alert processed after gap	8/29/2013	6:15 AM			3	3
Alert Gap	8/29/2013	7:00 PM	8/29/2013	7:00 PM	1	0
Alert processed after gap	8/29/2013	8:00 PM			1	1
Alert Gap	8/30/2013	12:00 AM	8/30/2013	4:00 AM	5	0
Alert processed after gap	8/30/2013	5:45 AM			43	43
Alert Gap	8/30/2013	7:00 PM	8/30/2013	7:00 PM	1	0
Alert processed after gap	8/30/2013	8:00 PM			2	2
Alert Gap	8/31/2013	2:00 PM	8/31/2013	7:00 PM	6	0
Alert processed after gap	8/31/2013	8:45 PM			6	6
Alert Gap	8/31/2013	9:00 PM	8/31/2013	10:00 PM	2	0
Alert processed after gap	8/31/2013	11:00 PM			22	22
Alert Gap	9/1/2013	5:00 AM	9/1/2013	7:00 AM	3	0
Alert processed after gap	9/1/2013	8:00 AM			1	1
Alert Gap	9/1/2013	9:00 AM	9/1/2013	9:00 AM	1	0
Alert processed after gap	9/1/2013	10:15 AM			1	1
Alert Gap	9/1/2013	11:00 AM	9/1/2013	12:00 PM	2	0
Alert processed after gap	9/1/2013	1:15 PM			1	1
Alert Gap	9/1/2013	2:00 PM	9/1/2013	3:00 PM	2	0
Alert processed after gap	9/1/2013	4:15 PM			113	99
Alert Gap	9/1/2013	5:00 PM	9/2/2013	5:00 AM	13	0
Alert processed after gap	9/2/2013	6:00 AM			3	3

(b)(3);6(f);b(4)

Alert Gap	9/2/2013	8:00 AM	9/2/2013	12:00 PM	5	0		
Alert processed after gap	9/2/2013	1:00 PM				1	1	
Alert Gap	9/2/2013	2:00 PM	9/2/2013	2:00 PM	1	0		
Alert processed after gap	9/2/2013	3:30 PM				1	1	
Alert Gap	9/2/2013	4:00 PM	9/2/2013	4:00 PM	1	0		
Alert processed after gap	9/2/2013	5:30 PM				1	1	
Alert Gap	9/2/2013	7:00 PM	9/2/2013	8:00 PM	2	0		
Alert processed after gap	9/2/2013	8:15 PM				1	1	
Alert Gap	9/2/2013	9:00 PM	9/2/2013	10:00 PM	2	0		
Alert processed after gap	9/2/2013	11:00 PM				29	29	
Alert Gap	9/3/2013	12:00 AM	9/3/2013	4:00 AM	5	0		
Alert processed after gap	9/3/2013	5:45 AM				2	2	
Alert Gap	9/3/2013	7:00 PM	9/3/2013	7:00 PM	1	0		
Alert processed after gap	9/3/2013	8:00 PM				3	3	
Alert Gap	9/3/2013	9:00 PM	9/4/2013	5:00 AM	9	0		
Alert processed after gap	9/4/2013	6:15 AM				376	376	
Alert Gap	9/4/2013	7:00 PM	9/4/2013	7:00 PM	1	0		
Alert processed after gap	9/4/2013	8:00 PM				1	1	
Alert Gap	9/5/2013	2:00 AM	9/5/2013	2:00 AM	1	0		
Alert processed after gap	9/5/2013	3:30 AM				8	8	
Alert Gap	9/5/2013	7:00 PM	9/5/2013	7:00 PM	1	0		
Alert processed after gap	9/5/2013	8:00 PM				2	2	
Alert Gap	9/5/2013	9:00 PM	9/6/2013	5:00 AM	9	0		
Alert processed after gap	9/6/2013	6:15 AM				251	251	
Alert Gap	9/7/2013	4:00 AM	9/7/2013	4:00 AM	1	0		
Alert processed after gap	9/7/2013	5:30 AM				57	55	
Alert Gap	9/7/2013	3:00 PM	9/7/2013	3:00 PM	1	0		
Alert processed after gap	9/7/2013	4:00 PM				1	1	
Alert Gap	9/7/2013	5:00 PM	9/7/2013	9:00 PM	5	0		
Alert processed after gap	9/7/2013	10:45 PM				1	1	
Alert Gap	9/8/2013	7:00 AM	9/8/2013	2:00 PM	8	0		

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

Alert processed after gap	9/8/2013	3:30 PM			1	1
Alert Gap	9/8/2013	4:00 PM	9/9/2013	5:00 AM	14	0
Alert processed after gap	9/9/2013	6:00 AM			3	3
Alert Gap	9/9/2013	7:00 PM	9/9/2013	7:00 PM	1	0
Alert processed after gap	9/9/2013	8:15 PM			1	1
Alert Gap	9/10/2013	3:00 AM	9/10/2013	3:00 AM	1	0
Alert processed after gap	9/10/2013	4:00 AM			12	12
Alert Gap	9/10/2013	7:00 PM	9/10/2013	7:00 PM	1	0
Alert processed after gap	9/10/2013	8:00 AM			2	2
Alert Gap	9/10/2013	9:00 PM	9/11/2013	5:00 AM	9	0
Alert processed after gap	9/11/2013	6:00 AM			214	213
Alert Gap	9/11/2013	8:00 PM	9/11/2013	8:00 PM	1	0
Alert processed after gap	9/11/2013	9:00 PM			14	14
Alert Gap	9/12/2013	5:00 PM	9/12/2013	5:00 PM	1	0
Alert processed after gap	9/12/2013	6:00 PM			20	20
Alert Gap	9/12/2013	7:00 PM	9/12/2013	7:00 PM	1	0
Alert processed after gap	9/12/2013	8:00 PM			2	2
Alert Gap	9/12/2013	9:00 PM	9/13/2013	5:00 AM	9	0
Alert processed after gap	9/13/2013	6:00 AM			88	88
Alert Gap	9/13/2013	8:00 AM	9/13/2013	9:00 AM	2	0
Alert processed after gap	9/13/2013	10:00 AM			11	11
Alert Gap	9/13/2013	7:00 PM	9/13/2013	8:00 PM	2	0
Alert processed after gap	9/13/2013	9:00 PM			3	3
Alert Gap	9/14/2013	12:00 AM	9/14/2013	12:00 AM	1	0
Alert processed after gap	9/14/2013	1:15 AM			10	10
Alert Gap	9/14/2013	3:00 AM	9/14/2013	3:00 AM	1	0
Alert processed after gap	9/14/2013	4:30 AM			5	5
Alert Gap	9/14/2013	5:00 AM	9/14/2013	5:00 AM	1	0
Alert processed after gap	9/14/2013	6:30 AM			1	1
Alert Gap	9/14/2013	9:00 AM	9/14/2013	9:00 AM	1	0
Alert processed after gap	9/14/2013	10:45 AM			3	3

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

Alert Gap	9/14/2013	12:00 PM	9/14/2013	12:00 PM	1	0	
Alert processed after gap	9/14/2013	1:00 PM				1	1
Alert Gap	9/14/2013	4:00 PM	9/14/2013	6:00 PM	3	0	
Alert processed after gap	9/14/2013	7:15 PM				6	5
Alert Gap	9/14/2013	9:00 PM	9/14/2013	10:00 PM	2	0	
Alert processed after gap	9/14/2013	11:00 PM				20	20
Alert Gap	9/15/2013	12:00 AM	9/15/2013	12:00 AM	1	0	
Alert processed after gap	9/15/2013	1:15 AM				1	1
Alert Gap	9/15/2013	2:00 AM	9/15/2013	8:00 AM	7	0	
Alert processed after gap	9/15/2013	9:15 AM				1	1
Alert Gap	9/15/2013	10:00 AM	9/15/2013	10:00 AM	1	0	
Alert processed after gap	9/15/2013	11:00 AM				1	1
Alert Gap	9/15/2013	12:00 PM	9/15/2013	1:00 PM	2	0	
Alert processed after gap	9/15/2013	2:45 PM				1	1
Alert Gap	9/15/2013	3:00 PM	9/16/2013	5:00 AM	15	0	
Alert processed after gap	9/16/2013	6:00 AM				1	1
Alert Gap	9/16/2013	7:00 PM	9/16/2013	7:00 PM	1	0	
Alert processed after gap	9/16/2013	8:00 PM				1	1
Alert Gap	9/17/2013	12:00 AM	9/17/2013	12:00 AM	1	0	
Alert processed after gap	9/17/2013	1:30 AM				3	3
Alert Gap	9/17/2013	2:00 AM	9/17/2013	2:00 AM	1	0	
Alert processed after gap	9/17/2013	3:15 AM				8	8
Alert Gap	9/17/2013	7:00 PM	9/17/2013	7:00 PM	1	0	
Alert processed after gap	9/17/2013	8:15 PM				1	1
Alert Gap	9/17/2013	9:00 PM	9/18/2013	5:00 AM	9	0	
Alert processed after gap	9/18/2013	6:00 AM				147	147
Alert Gap	9/18/2013	7:00 PM	9/18/2013	8:00 PM	2	0	
Alert processed after gap	9/18/2013	9:00 PM				14	14
Alert Gap	9/19/2013	2:00 AM	9/19/2013	2:00 AM	1	0	
Alert processed after gap	9/19/2013	3:15 AM				2	2
Alert Gap	9/19/2013	4:00 AM	9/19/2013	5:00 AM	2	0	

(b)(3);6(f);(b)(4)

Alert processed after gap	9/19/2013	6:00 AM			1	1
Alert Gap	9/20/2013	2:00 AM	9/20/2013	2:00 AM	1	0
Alert processed after gap	9/20/2013	3:30 AM			7	7
Alert Gap	9/20/2013	5:00 PM	9/20/2013	5:00 PM	1	0
Alert processed after gap	9/20/2013	6:15 PM			28	28
Alert Gap	9/20/2013	7:00 PM	9/20/2013	7:00 PM	1	0
Alert processed after gap	9/20/2013	8:15 PM			3	3
Alert Gap	9/21/2013	7:00 PM	9/21/2013	7:00 PM	1	0
Alert processed after gap	9/21/2013	8:00 PM			2	2
Alert Gap	9/21/2013	9:00 PM	9/21/2013	9:00 PM	1	0
Alert processed after gap	9/21/2013	10:45 PM			3	3
Alert Gap	9/22/2013	4:00 AM	9/22/2013	5:00 AM	2	0
Alert processed after gap	9/22/2013	6:00 AM			80	72
Alert Gap	9/22/2013	10:00 AM	9/22/2013	10:00 AM	1	0
Alert processed after gap	9/22/2013	11:30 AM			1	1
Alert Gap	9/22/2013	1:00 PM	9/22/2013	3:00 PM	3	0
Alert processed after gap	9/22/2013	4:45 PM			41	40
Alert Gap	9/22/2013	5:00 PM	9/22/2013	5:00 PM	1	0
Alert processed after gap	9/22/2013	6:30 PM			2	2
Alert Gap	9/22/2013	7:00 PM	9/23/2014	12:00 AM	6	0
Alert processed after gap	9/23/2013	1:00 AM			1	1
Alert Gap	9/23/2013	2:00 AM	9/23/2013	5:00 AM	4	0
Alert processed after gap	9/23/2013	6:00 AM			6	6
Alert Gap	9/23/2013	7:00 PM	9/23/2013	8:00 PM	2	0
Alert processed after gap	9/23/2013	9:00 PM			4	4
Alert Gap	9/24/2013	2:00 AM	9/24/2013	2:00 AM	1	0
Alert processed after gap	9/24/2013	3:30 AM			14	14
Alert Gap	9/24/2013	7:00 PM	9/24/2013	7:00 PM	1	0
Alert processed after gap	9/24/2013	8:00 PM			1	1
Alert Gap	9/24/2013	9:00 PM	9/25/2013	5:00 AM	9	0
Alert processed after gap	9/25/2013	6:00 AM			96	96

(b)(3);6(f);(b)(4)

Alert Gap	9/25/2013	5:00 PM	9/25/2013	5:00 PM	1	0
Alert processed after gap	9/25/2013	6:15 PM				15
Alert Gap	9/25/2013	7:00 PM	9/25/2013	7:00 PM	1	0
Alert processed after gap	9/25/2013	8:45 PM				16
Alert Gap	9/26/2013	2:00 AM	9/26/2013	2:00 AM	1	0
Alert processed after gap	9/26/2013	3:15 AM				2
Alert Gap	9/26/2013	4:00 AM	9/26/2013	5:00 AM	2	0
Alert processed after gap	9/26/2013	6:00 AM				1
Alert Gap	9/26/2013	5:00 PM	9/26/2013	5:00 PM	1	0
Alert processed after gap	9/26/2013	6:00 PM				3
Alert Gap	9/26/2013	7:00 PM	9/26/2013	7:00 PM	1	0
Alert processed after gap	9/26/2013	8:00 PM				2
Alert Gap	9/26/2013	9:00 PM	9/27/2013	5:00 AM	9	0
Alert processed after gap	9/27/2013	6:15 AM				3
Alert Gap	9/27/2013	7:00 PM	9/27/2013	8:00 PM	2	0
Alert processed after gap	9/27/2013	9:00 PM				15
Alert Gap	9/28/2013	4:00 AM	9/28/2013	4:00 AM	1	0
Alert processed after gap	9/28/2013	5:00 AM				3
Alert Gap	9/28/2013	2:00 PM	9/28/2013	2:00 PM	1	0
Alert processed after gap	9/28/2013	3:45 PM				1
Alert Gap	9/28/2013	5:00 PM	9/28/2013	7:00 PM	3	0
Alert processed after gap	9/28/2013	8:00 PM				1
Alert Gap	9/29/2013	4:00 AM	9/29/2013	4:00 AM	1	0
Alert processed after gap	9/29/2013	5:45 AM				39
Alert Gap	9/29/2013	12:00 PM	9/29/2013	1:00 PM	2	0
Alert processed after gap	9/29/2013	2:00 PM				38
Alert Gap	9/29/2013	3:00 PM	9/29/2013	5:00 PM	3	0
Alert processed after gap	9/29/2013	6:15 PM				1
Alert Gap	9/29/2013	7:00 PM	9/29/2013	9:00 PM	3	0
Alert processed after gap	9/29/2013	10:00 PM				1
Alert Gap	9/29/2013	11:00 PM	9/30/2013	12:00 AM	2	0

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

Alert processed after gap	9/30/2013	1:30 AM			1	1
Alert Gap	9/30/2013	2:00 AM	9/30/2013	5:00 AM	4	0
Alert processed after gap	9/30/2013	6:00 AM			3	3
Alert Gap	9/30/2013	7:00 PM	9/30/2013	8:00 PM	2	0
Alert processed after gap	9/30/2013	9:00 PM			3	3
Alert Gap	10/1/2013	7:00 PM	10/2/2013	4:00 AM	10	0
Alert processed after gap	10/2/2013	5:30 AM			3	3
Alert Gap	10/3/2013	2:00 AM	10/3/2013	2:00 AM	1	0
Alert processed after gap	10/3/2013	3:30 AM			17	16
Alert Gap	10/3/2013	5:00 AM	10/3/2013	5:00 AM	1	0
Alert processed after gap	10/3/2013	6:00 AM			1	1
Alert Gap	10/3/2013	7:00 PM	10/3/2013	7:00 PM	1	0
Alert processed after gap	10/3/2013	8:00 PM			2	2
Alert Gap	10/4/2013	5:00 AM	10/4/2013	5:00 AM	1	0
Alert processed after gap	10/4/2013	6:45 AM			2	2
Alert Gap	10/4/2013	7:00 PM	10/4/2013	7:00 PM	1	0
Alert processed after gap	10/4/2013	8:00 PM	10/4/2013		3	3
Alert Gap	10/5/2013	6:00 AM	10/5/2013	6:00 AM	1	0
Alert processed after gap	10/5/2013	7:00 AM			2	2
Alert Gap	10/5/2013	7:00 PM	10/5/2013	7:00 PM	1	0
Alert processed after gap	10/5/2013	8:00 PM			1	1
Alert Gap	10/5/2013	9:00 PM	10/5/2013	10:00 PM	2	0
Alert processed after gap	10/5/2013	11:00 PM			34	34
Alert Gap	10/6/2013	8:00 AM	10/6/2013	12:00 PM	5	0
Alert processed after gap	10/6/2013	1:45 PM			63	57
Alert Gap	10/6/2013	3:00 PM	10/6/2013	5:00 PM	3	0
Alert processed after gap	10/6/2013	6:30 PM			1	1
Alert Gap	10/6/2013	7:00 PM	10/6/2013	9:00 PM	3	0
Alert processed after gap	10/6/2013	10:15 PM			1	1
Alert Gap	10/6/2013	11:00 PM	10/7/2013	6:00 AM	8	0
Alert processed after gap	10/7/2013	7:00 AM			2	2

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

Alert Gap	10/7/2013	7:00 PM	10/7/2013	7:00 PM	1	0
Alert processed after gap	10/7/2013	8:00 PM				1
Alert Gap	10/8/2013	2:00 AM	10/8/2013	2:00 AM	1	0
Alert processed after gap	10/8/2013	3:30 AM				1
Alert Gap	10/8/2013	5:00 AM	10/8/2013	5:00 AM	1	0
Alert processed after gap	10/8/2013	6:30 AM				7
Alert Gap	10/8/2013	5:00 PM	10/8/2013	5:00 PM	1	0
Alert processed after gap	10/8/2013	6:00 PM				22
Alert Gap	10/8/2013	7:00 PM	10/8/2013	7:00 PM	1	0
Alert processed after gap	10/8/2013	8:00 PM				5
Alert Gap	10/9/2013	5:00 AM	10/9/2013	5:00 AM	1	0
Alert processed after gap	10/9/2013	6:00 AM				1
Alert Gap	10/9/2013	7:00 PM	10/9/2013	7:00 PM	1	0
Alert processed after gap	10/9/2013	8:00 PM				1
Alert Gap	10/10/2013	2:00 AM	10/10/2013	2:00 AM	1	0
Alert processed after gap	10/10/2013	3:30 AM				11
Alert Gap	10/10/2013	5:00 AM	10/10/2013	5:00 AM	1	0
Alert processed after gap	10/10/2013	6:15 AM				1
Alert Gap	10/10/2013	9:00 AM	10/10/2013	9:00 AM	1	0
Alert processed after gap	10/10/2013	10:00 AM				2
Alert Gap	10/10/2013	7:00 PM	10/10/2013	7:00 PM	1	0
Alert processed after gap	10/10/2013	8:00 PM				1
Alert Gap	10/11/2013	2:00 AM	10/11/2013	2:00 AM	1	0
Alert processed after gap	10/11/2013	3:00 AM				1
Alert Gap	10/11/2013	5:00 PM	10/11/2013	5:00 PM	1	0
Alert processed after gap	10/11/2013	6:00 PM				12
Alert Gap	10/11/2013	7:00 PM	10/11/2013	8:00 PM	2	0
Alert processed after gap	10/11/2013	9:00 PM				21
Alert Gap	10/12/2013	6:00 AM	10/12/2013	6:00 AM	1	0
Alert processed after gap	10/12/2013	7:00 AM				1
Alert Gap	10/12/2013	2:00 PM	10/12/2013	2:00 PM	1	0

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

Alert processed after gap	10/12/2013	3:30 PM			2	2
Alert Gap	10/12/2013	8:00 PM	10/12/2013	10:00 PM	3	0
Alert processed after gap	10/12/2013	11:00 PM			33	33
Alert Gap	10/13/2013	12:00 AM	10/13/2013	3:00 AM	4	0
Alert processed after gap	10/13/2013	4:00 AM			3	2
Alert Gap	10/13/2013	9:00 AM	10/13/2013	11:00 AM	3	0
Alert processed after gap	10/13/2013	12:45 PM			1	1
Alert Gap	10/13/2013	1:00 PM	10/13/2013	2:00 PM	2	0
Alert processed after gap	10/13/2013	3:00 PM			1	1
Alert Gap	10/13/2013	4:00 PM	10/13/2013	4:00 PM	1	0
Alert processed after gap	10/13/2013	5:45 PM			1	1
Alert Gap	10/13/2013	6:00 PM	10/14/2013	5:00 AM	12	0
Alert processed after gap	10/14/2013	6:15 AM			2	2
Alert Gap	10/14/2013	6:00 PM	10/14/2013	6:00 PM	1	0
Alert processed after gap	10/14/2013	7:30 PM			2	2
Alert Gap	10/14/2013	10:00 PM	10/14/2013	10:00 PM	1	0
Alert processed after gap	10/14/2013	11:15 PM			91	91
Alert Gap	10/15/2013	12:00 AM	10/15/2013	12:00 AM	1	0
Alert processed after gap	10/15/2013	1:30 AM			3	3
Alert Gap	10/15/2013	2:00 AM	10/15/2013	4:00 AM	3	0
Alert processed after gap	10/15/2013	5:30 AM			1	1
Alert Gap	10/15/2013	4:00 PM	10/15/2013	4:00 PM	1	0
Alert processed after gap	10/15/2013	5:00 PM			2	2
Alert Gap	10/15/2013	7:00 PM	10/15/2013	7:00 PM	1	0
Alert processed after gap	10/15/2013	8:00 PM			1	1
Alert Gap	10/16/2013	2:00 AM	10/16/2013	3:00 AM	2	0
Alert processed after gap	10/16/2013	4:30 AM			13	13
Alert Gap	10/16/2013	5:00 AM	10/16/2013	5:00 AM	1	0
Alert processed after gap	10/16/2013	6:00 AM			1	1
Alert Gap	10/17/2013	2:00 AM	10/17/2013	2:00 AM	1	0
Alert processed after gap	10/17/2013	3:30 AM			7	7

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

Alert Gap	10/17/2013	4:00 AM	10/17/2013	4:00 AM	1	0	(b)(3);6(f),(b)(4)	
Alert processed after gap	10/17/2013	5:45 AM				3		3
Alert Gap	10/17/2013	7:00 PM	10/17/2013	7:00 PM	1	0		
Alert processed after gap	10/17/2013	8:00 PM				2		2
Alert Gap	10/17/2013	11:00 PM	10/18/2013	1:00 PM	3	0		
Alert processed after gap	10/18/2013	2:00 AM				119		119
Alert Gap	10/18/2013	7:00 PM	10/18/2013	7:00 PM	1	0		
Alert processed after gap	10/18/2013	8:00 PM				2		2
Alert Gap	10/19/2013	10:00 AM	10/19/2013	10:00 AM	1	0		
Alert processed after gap	10/19/2013	11:00 AM				1		1
Alert Gap	10/19/2013	2:00 PM	10/19/2013	3:00 PM	2	0		
Alert processed after gap	10/19/2013	4:15 PM				2		2
Alert Gap	10/19/2013	7:00 PM	10/19/2013	7:00 PM	1	0		
Alert processed after gap	10/19/2013	8:45 PM				71		63
Alert Gap	10/19/2013	9:00 PM	10/19/2013	9:00 PM	1	0		
Alert processed after gap	10/19/2013	10:45 PM				2		1
Alert Gap	10/20/2013	4:00 AM	10/20/2013	5:00 AM	2	0		
Alert processed after gap	10/20/2013	6:00 AM				71		67
Alert Gap	10/20/2013	7:00 AM	10/20/2013	7:00 AM	1	0		
Alert processed after gap	10/20/2013	8:30 AM				28		27
Alert Gap	10/20/2013	11:00 AM	10/20/2013	2:00 PM	4	0		
Alert processed after gap	10/20/2013	3:15 PM				1		1
Alert Gap	10/20/2013	5:00 PM	10/20/2013	5:00 PM	1	0		
Alert processed after gap	10/20/2013	6:15 PM				1		1
Alert Gap	10/20/2013	8:00 PM	10/21/2013	4:00 AM	9	0		
Alert processed after gap	10/21/2013	5:45 AM				1		1
Alert Gap	10/21/2013	9:00 PM	10/21/2013	9:00 PM	1	0		
Alert processed after gap	10/21/2013	10:15 PM				109		109
Alert Gap	10/22/2013	4:00 AM	10/22/2013	4:00 AM	1	0		
Alert processed after gap	10/22/2013	5:00 AM				1		1
Alert Gap	10/22/2013	5:00 PM	10/22/2013	5:00 PM	1	0		

Alert processed after gap	10/22/2013	6:00 PM			1	1
Alert Gap	10/23/2013	2:00 AM	10/23/2013	2:00 AM	1	0
Alert processed after gap	10/23/2013	3:00 AM			1	1
Alert Gap	10/23/2013	4:00 AM	10/23/2013	4:00 AM	1	0
Alert processed after gap	10/23/2013	5:00 AM			1	1
Alert Gap	10/23/2013	5:00 PM	10/23/2013	8:00 PM	4	0
Alert processed after gap	10/23/2013	9:00 PM			20	20
Alert Gap	10/24/2013	5:00 AM	10/24/2013	5:00 AM	1	0
Alert processed after gap	10/24/2013	6:00 AM			1	1
Alert Gap	10/24/2013	7:00 PM	10/25/2013	5:00 AM	11	0
Alert processed after gap	10/25/2013	6:15 AM			139	139
Alert Gap	10/25/2013	7:00 PM	10/25/2013	9:00 PM	3	0
Alert processed after gap	10/25/2013	10:15 PM			88	88
Alert Gap	10/26/2013	4:00 AM	10/26/2013	4:00 AM	1	0
Alert processed after gap	10/26/2013	5:30 AM			2	2
Alert Gap	10/26/2013	11:00 AM	10/26/2013	11:00 AM	1	0
Alert processed after gap	10/26/2013	12:00 PM			1	1
Alert Gap	10/26/2013	5:00 PM	10/26/2013	5:00 PM	1	0
Alert processed after gap	10/26/2013	6:00 PM			61	56
Alert Gap	10/26/2013	7:00 PM	10/27/2013	12:00 AM	6	0
Alert processed after gap	10/27/2013	1:15 AM			175	162
Alert Gap	10/27/2013	4:00 AM	10/27/2013	4:00 AM	1	0
Alert processed after gap	10/27/2013	5:15 AM			57	50
Alert Gap	10/27/2013	9:00 AM	10/27/2013	12:00 PM	4	0
Alert processed after gap	10/27/2013	1:15 PM			1	1
Alert Gap	10/27/2013	2:00 PM	10/27/2013	2:00 PM	1	0
Alert processed after gap	10/27/2013	3:00 PM			62	51
Alert Gap	10/27/2013	4:00 PM	10/28/2013	5:00 AM	14	0
Alert processed after gap	10/28/2013	6:00 AM			6	6
Alert Gap	10/29/2013	5:00 AM	10/29/2013	5:00 AM	1	0
Alert processed after gap	10/29/2013	6:45 AM			2	2

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

Alert Gap	10/29/2013	9:00 AM	10/29/2013	9:00 AM	1	0
Alert processed after gap	10/29/2013	8:00 PM				3
Alert Gap	10/29/2013	9:00 PM	10/30/2013	5:00 AM	9	0
Alert processed after gap	10/30/2013	6:15 AM				314
Alert Gap	10/30/2013	7:00 PM	10/30/2013	8:00 PM	2	0
Alert processed after gap	10/30/2013	9:00 PM				6
Alert Gap	10/31/2013	2:00 AM	10/31/2013	2:00 AM	1	0
Alert processed after gap	10/31/2013	3:15 AM				2
Alert Gap	10/31/2013	7:00 PM	10/31/2013	7:00 PM	1	0
Alert processed after gap	10/31/2013	8:00 PM				1
Alert Gap	11/1/2013	3:00 AM	11/1/2013	3:00 AM	1	0
Alert processed after gap	11/1/2013	4:00 AM				5
Alert Gap	11/1/2013	5:00 AM	11/1/2013	5:00 AM	1	0
Alert processed after gap	11/1/2013	6:00 AM				7
Alert Gap	11/1/2013	7:00 PM	11/4/2013	8:00 AM	62	0
Alert processed after gap	11/4/2013	9:45 AM				209
Alert Gap	11/4/2013	8:00 PM	11/4/2013	8:00 PM	1	0
Alert processed after gap	11/4/2013	9:00 PM				1
Alert Gap	11/5/2013	6:00 PM	11/6/2013	7:00 AM	14	0
Alert processed after gap	11/6/2013	8:00 AM				278
Alert Gap	11/6/2013	6:00 PM	11/6/2013	6:00 PM	1	0
Alert processed after gap	11/6/2013	7:00 PM				1
Alert Gap	11/6/2013	8:00 PM	11/6/2013	9:00 PM	2	0
Alert processed after gap	11/6/2013	10:00 PM				4
Alert Gap	11/7/2013	2:00 AM	11/7/2013	3:00 AM	2	0
Alert processed after gap	11/7/2013	4:15 AM				5
Alert Gap	11/7/2013	5:00 AM	11/7/2013	5:00 AM	1	0
Alert processed after gap	11/7/2013	6:00 AM				1
Alert Gap	11/7/2013	6:00 PM	11/7/2013	6:00 PM	1	0
Alert processed after gap	11/7/2013	7:00 PM				1
Alert Gap	11/7/2013	8:00 PM	11/8/2013	7:00 AM	12	0

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

Alert processed after gap	11/8/2013	8:00 AM			267	267
Alert Gap	11/8/2013	7:00 PM	11/12/2013	6:00 AM	84	0
Alert processed after gap	11/13/2013	7:15 AM			74	74
Alert Gap	11/13/2013	9:00 PM	11/14/2013	5:00 AM	9	0
Alert processed after gap	11/14/2013	6:15 AM			131	131
Alert Gap	11/14/2013	8:00 AM	11/14/2013	8:00 AM	1	0
Alert processed after gap	11/14/2013	9:00 AM			1	1
Alert Gap	11/14/2013	8:00 PM	11/14/2013	8:00 PM	1	0
Alert processed after gap	11/14/2013	9:00 PM			2	2
Alert Gap	11/15/2013	2:00 AM	11/15/2013	2:00 AM	1	0
Alert processed after gap	11/15/2013	3:30 AM			10	10
Alert Gap	11/15/2013	8:00 PM	11/15/2013	8:00 PM	1	0
Alert processed after gap	11/15/2013	9:00 PM			4	4
Alert Gap	11/16/2013	3:00 PM	11/16/2013	6:00 PM	4	0
Alert processed after gap	11/16/2013	7:45 PM			1	1
Alert Gap	11/16/2013	8:00 PM	11/16/2013	10:00 PM	3	0
Alert processed after gap	11/16/2013	11:00 PM			20	18
Alert Gap	11/17/2013	5:00 AM	11/17/2013	6:00 AM	2	0
Alert processed after gap	11/17/2013	7:00 AM			79	77
Alert Gap	11/17/2013	8:00 AM	11/17/2013	11:00 AM	4	0
Alert processed after gap	11/17/2013	12:30 PM			107	94
Alert Gap	11/17/2013	1:00 PM	11/17/2013	1:00 PM	1	0
Alert processed after gap	11/17/2013	2:15 PM			49	43
Alert Gap	11/17/2013	4:00 PM	11/17/2013	4:00 PM	1	0
Alert processed after gap	11/17/2013	5:00 PM			15	14
Alert Gap	11/17/2013	7:00 PM	11/18/2013	6:00 AM	12	0
Alert processed after gap	11/18/2013	7:00 AM			5	5
Alert Gap	11/18/2013	8:00 PM	11/18/2013	9:00 PM	2	0
Alert processed after gap	11/18/2013	10:00 PM			1	1
Alert Gap	11/19/2013	6:00 AM	11/19/2013	6:00 AM	1	0

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

Alert processed after gap	11/19/2013	7:15 AM			1	1
Alert Gap	11/19/2013	8:00 PM	11/20/2013	5:00 AM	10	0
Alert processed after gap	11/20/2013	6:15 AM			187	187
Alert Gap	11/20/2013	9:00 AM	11/22/2013	12:00 PM	52	0
Alert processed after gap	11/22/2013	1:45 PM			218	207
Alert Gap	11/22/2013	9:00 PM	11/22/2013	9:00 PM	1	0
Alert processed after gap	11/22/2013	10:00 PM			1	1
Alert Gap	11/23/2013	3:00 AM	11/23/2013	3:00 AM	1	0
Alert processed after gap	11/23/2013	4:15 AM			122	114
Alert Gap	11/23/2013	7:00 AM	11/23/2013	8:00 AM	2	0
Alert processed after gap	11/23/2013	9:00 AM			1	1
Alert Gap	11/23/2013	8:00 PM	11/23/2013	8:00 PM	1	0
Alert processed after gap	11/23/2013	9:00 PM			56	50
Alert Gap	11/23/2013	10:00 PM	11/23/2013	10:00 PM	1	0
Alert processed after gap	11/23/2013	11:45 PM			1	1
Alert Gap	11/24/2013	8:00 AM	11/27/2013	8:00 AM	73	0
Alert processed after gap	11/27/2013	9:00 AM			195	187
Alert Gap	11/27/2013	4:00 PM	11/27/2013	4:00 PM	1	0
Alert processed after gap	11/27/2013	5:00 PM			1	1
Alert Gap	11/27/2013	6:00 PM	11/27/2013	6:00 PM	1	0
Alert processed after gap	11/27/2013	7:00 PM			15	15
Alert Gap	11/27/2013	8:00 PM	11/27/2013	8:00 PM	1	0
Alert processed after gap	11/27/2013	9:00 PM			1	1
Alert Gap	11/28/2013	3:00 AM	11/28/2013	3:00 AM	1	0
Alert processed after gap	11/28/2013	4:00 AM			5	5
Alert Gap	11/28/2013	6:00 AM	11/28/2013	8:00 AM	3	0
Alert processed after gap	11/28/2013	9:30 AM			1	1
Alert Gap	11/28/2013	10:00 AM	11/28/2013	1:00 PM	4	0
Alert processed after gap	11/28/2013	2:15 PM			1	1
Alert Gap	11/28/2013	3:00 PM	11/28/2013	7:00 PM	5	0

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

Alert processed after gap	11/28/2013	8:45 PM			1	1
Alert Gap	11/28/2013	9:00 PM	11/28/2013	11:00 PM	3	0
Alert processed after gap	11/29/2013	12:00 AM			59	59
Alert Gap	11/29/2013	1:00 AM	11/29/2013	6:00 AM	6	0
Alert processed after gap	11/29/2013	7:15 AM			1	1
Alert Gap	11/29/2013	5:00 PM	11/29/2013	6:00 PM	2	0
Alert processed after gap	11/29/2013	7:00 PM			11	11
Alert Gap	11/29/2013	8:00 PM	11/29/2013	8:00 PM	1	0
Alert processed after gap	11/29/2013	9:00 PM			6	6
Alert Gap	11/30/2013	9:00 PM	11/30/2013	10:00 PM	2	0
Alert processed after gap	11/30/2013	11:45 PM			1	1
Alert Gap	12/1/2013	6:00 AM	12/1/2013	6:00 AM	1	0
Alert processed after gap	12/1/2013	7:00 AM			77	74
Alert Gap	12/1/2013	9:00 AM	12/1/2013	9:00 AM	1	0
Alert processed after gap	12/1/2013	10:00 AM			1	1
Alert Gap	12/1/2013	11:00 AM	12/1/2013	1:00 PM	3	0
Alert processed after gap	12/1/2013	2:45 PM			41	36
Alert Gap	12/1/2013	4:00 PM	12/1/2013	5:00 PM	2	0
Alert processed after gap	12/1/2013	6:00 PM			1	1
Alert Gap	12/1/2013	7:00 PM	12/2/2013	5:00 AM	11	0
Alert processed after gap	12/2/2013	6:30 AM			1	1
Alert Gap	12/2/2013	8:00 PM	12/2/2013	9:00 PM	2	0
Alert processed after gap	12/2/2013	10:00 PM			22	22
Alert Gap	12/3/2013	6:00 AM	12/3/2013	6:00 AM	1	0
Alert processed after gap	12/3/2013	7:30 AM			1	1
Alert Gap	12/3/2013	6:00 PM	12/3/2013	6:00 PM	1	0
Alert processed after gap	12/3/2013	7:15 PM			18	18
Alert Gap	12/3/2013	8:00 PM	12/3/2013	8:00 PM	1	0
Alert processed after gap	12/3/2013	9:00 PM			2	2
Alert Gap	12/4/2013	5:00 AM	12/4/2013	5:00 AM	1	0
Alert processed after gap	12/4/2013	6:00 AM			2	2

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

Alert Gap	12/4/2013	8:00 PM	12/4/2013	8:00 PM	1	0	
Alert processed after gap	12/4/2013	9:00 PM				1	1
Alert Gap	12/5/2013	5:00 AM	12/5/2013	5:00 AM	1	0	
Alert processed after gap	12/5/2013	6:00 AM				3	3
Alert Gap	12/5/2013	8:00 PM	12/6/2013	5:00 AM	10	0	
Alert processed after gap	12/6/2013	6:00 AM				189	189
Alert Gap	12/6/2013	9:00 PM	12/7/2013	12:00 AM	4	0	
Alert processed after gap	12/7/2013	1:15 AM				45	45
Alert Gap	12/7/2013	2:00 PM	12/7/2013	3:00 PM	2	0	
Alert processed after gap	12/7/2013	4:00 PM				1	1
Alert Gap	12/7/2013	5:00 PM	12/7/2013	8:00 PM	4	0	
Alert processed after gap	12/7/2013	9:00 PM				2	2
Alert Gap	12/8/2013	5:00 AM	12/8/2013	6:00 AM	2	0	
Alert processed after gap	12/8/2013	7:00 AM				93	89
Alert Gap	12/8/2013	8:00 AM	12/8/2013	11:00 AM	4	0	
Alert processed after gap	12/8/2013	12:30 PM				1	1
Alert Gap	12/8/2013	1:00 PM	12/8/2013	2:00 PM	2	0	
Alert processed after gap	12/8/2013	3:45 PM				1	1
Alert Gap	12/8/2013	5:00 PM	12/8/2013	6:00 PM	2	0	
Alert processed after gap	12/8/2013	7:15 PM				31	28
Alert Gap	12/8/2013	8:00 PM	12/9/2013	6:00 AM	11	0	
Alert processed after gap	12/9/2013	7:00 AM				4	4
Alert Gap	12/9/2013	10:00 AM	12/9/2013	10:00 AM	1	0	
Alert processed after gap	12/9/2013	11:00 AM				2	2
Alert Gap	12/9/2013	8:00 PM	12/9/2013	8:00 PM	1	0	
Alert processed after gap	12/9/2013	9:00 PM				1	1
Alert Gap	12/10/2013	7:00 AM	12/10/2013	7:00 AM	1	0	
Alert processed after gap	12/10/2013	8:00 AM				3	3
Alert Gap	12/10/2013	5:00 PM	12/10/2013	6:00 PM	2	0	
Alert processed after gap	12/10/2013	7:00 PM				15	15
Alert Gap	12/10/2013	8:00 PM	12/11/2013	3:00 AM	8	0	

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

Alert processed after gap	12/11/2013	4:45 AM				330	330
Alert Gap	12/11/2013	5:00 AM	12/11/2013	5:00 AM	1	0	
Alert processed after gap	12/11/2013	6:15 AM				3	3
Alert Gap	12/11/2013	6:00 PM	12/11/2013	6:00 PM	1	0	
Alert processed after gap	12/11/2013	7:15 PM				13	13
Alert Gap	12/11/2013	8:00 PM	12/12/2013	5:00 AM	10	0	
Alert processed after gap	12/12/2013	6:30 AM				229	225
Alert Gap	12/12/2013	11:00 AM	12/12/2013	11:00 AM	1	0	
Alert processed after gap	12/12/2013	12:00 PM				25	25
Alert Gap	12/12/2013	6:00 PM	12/12/2013	6:00 PM	1	0	
Alert processed after gap	12/12/2013	7:00 PM				9	9
Alert Gap	12/12/2013	9:00 PM	12/13/2013	6:00 AM	10	0	
Alert processed after gap	12/13/2013	7:00 AM				263	262
Alert Gap	12/13/2013	8:00 PM	12/13/2013	8:00 PM	1	0	
Alert processed after gap	12/13/2013	9:00 PM				1	1
Alert Gap	12/14/2013	8:00 PM	12/14/2013	8:00 PM	1	0	
Alert processed after gap	12/14/2013	9:00 PM				185	176
Alert Gap	12/14/2013	10:00 PM	12/14/2013	10:00 PM	1	0	
Alert processed after gap	12/14/2013	11:30 PM				3	3
Alert Gap	12/15/2013	5:00 AM	12/15/2013	5:00 AM	1	0	
Alert processed after gap	12/15/2013	6:45 AM				2	2
Alert Gap	12/15/2013	11:00 AM	12/15/2013	3:00 PM	5	0	
Alert processed after gap	12/15/2013	4:00 PM				57	53
Alert Gap	12/15/2013	5:00 PM	12/15/2013	6:00 PM	2	0	
Alert processed after gap	12/15/2013	7:15 PM				1	1
Alert Gap	12/15/2013	9:00 PM	12/15/2013	10:00 PM	2	0	
Alert processed after gap	12/15/2013	11:00 PM				1	1
Alert Gap	12/16/2013	12:00 AM	12/16/2013	2:00 AM	3	0	
Alert processed after gap	12/16/2013	3:15 AM				1	1
Alert Gap	12/16/2013	4:00 AM	12/16/2013	4:00 AM	1	0	
Alert processed after gap	12/16/2013	5:00 AM				1	1

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

Alert Gap	12/16/2013	6:00 AM	12/16/2013	6:00 AM	1	0	
Alert processed after gap	12/16/2013	7:00 AM				10	10
Alert Gap	12/16/2013	10:00 PM	12/17/2013	7:00 AM	10	0	
Alert processed after gap	12/17/2013	8:45 AM				300	300
Alert Gap	12/17/2013	6:00 PM	12/17/2013	6:00 PM	1	0	
Alert processed after gap	12/17/2013	7:00 PM				10	10
Alert Gap	12/17/2013	8:00 PM	12/17/2013	8:00 PM	1	0	
Alert processed after gap	12/17/2013	9:00 PM				3	3
Alert Gap	12/18/2013	3:00 AM	12/18/2013	3:00 AM	1	0	
Alert processed after gap	12/18/2013	4:00 AM				5	5
Alert Gap	12/18/2013	5:00 AM	12/18/2013	5:00 AM	1	0	
Alert processed after gap	12/18/2013	6:00 AM				2	2
Alert Gap	12/18/2013	8:00 PM	12/18/2013	9:00 PM	2	0	
Alert processed after gap	12/18/2013	10:00 PM				14	14
Alert Gap	12/19/2013	3:00 AM	12/19/2013	3:00 AM	1	0	
Alert processed after gap	12/19/2013	4:00 AM				4	4
Alert Gap	12/20/2013	5:00 AM	12/20/2013	6:00 AM	2	0	
Alert processed after gap	12/20/2013	7:00 AM				6	6
Alert Gap	12/20/2013	6:00 PM	12/20/2013	6:00 PM	1	0	
Alert processed after gap	12/20/2013	7:00 PM				2	2
Alert Gap	12/21/2013	7:00 PM	12/21/2013	7:00 PM	1	0	
Alert processed after gap	12/21/2013	8:00 PM				86	78
Alert Gap	12/22/2013	5:00 AM	12/22/2013	9:00 AM	5	0	
Alert processed after gap	12/22/2013	10:30 AM				217	195
Alert Gap	12/22/2013	12:00 PM	12/22/2013	2:00 PM	3	0	
Alert processed after gap	12/22/2013	3:15 PM				53	48
Alert Gap	12/22/2013	4:00 PM	12/22/2013	5:00 PM	2	0	
Alert processed after gap	12/22/2013	6:00 PM				1	1
Alert Gap	12/22/2013	8:00 PM	12/22/2013	11:00 PM	4	0	
Alert processed after gap	12/23/2013	12:45 AM				1	1
Alert Gap	12/23/2013	1:00 AM	12/23/2013	1:00 AM	1	0	

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

Alert processed after gap	12/23/2013	2:15 AM			1	1
Alert Gap	12/23/2013	3:00 AM	12/23/2013	5:00 AM	3	0
Alert processed after gap	12/23/2013	6:45 AM			1	1
Alert Gap	12/23/2013	8:00 PM	12/23/2013	9:00 PM	2	0
Alert processed after gap	12/23/2013	10:00 PM			19	19
Alert Gap	12/24/2013	3:00 AM	12/24/2013	3:00 AM	1	0
Alert processed after gap	12/24/2013	4:45 AM			47	47
Alert Gap	12/24/2013	6:00 AM	12/24/2013	6:00 AM	1	0
Alert processed after gap	12/24/2013	7:00 AM			1	1
Alert Gap	12/24/2013	4:00 PM	12/24/2013	6:00 PM	3	0
Alert processed after gap	12/24/2013	7:00 PM			10	10
Alert Gap	12/24/2013	8:00 PM	12/24/2013	8:00 PM	1	0
Alert processed after gap	12/24/2013	9:45 PM			8	8
Alert Gap	12/25/2013	2:00 AM	12/25/2013	2:00 AM	1	0
Alert processed after gap	12/25/2013	3:15 AM			1	1
Alert Gap	12/25/2013	12:00 PM	12/25/2013	12:00 PM	1	0
Alert processed after gap	12/25/2013	1:00 PM			1	1
Alert Gap	12/25/2013	2:00 PM	12/25/2013	7:00 PM	6	0
Alert processed after gap	12/25/2013	8:00 PM			1	1
Alert Gap	12/25/2013	9:00 PM	12/26/2013	12:00 AM	4	0
Alert processed after gap	12/26/2013	1:00 AM			63	63
Alert Gap	12/26/2013	2:00 AM	12/26/2013	4:00 AM	3	0
Alert processed after gap	12/26/2013	5:00 AM			1	1
Alert Gap	12/26/2013	6:00 AM	12/26/2013	6:00 AM	1	0
Alert processed after gap	12/26/2013	7:00 AM			1	1
Alert Gap	12/27/2013	3:00 AM	12/27/2013	3:00 AM	1	0
Alert processed after gap	12/27/2013	4:00 AM			2	2
Alert Gap	12/27/2013	5:00 AM	12/27/2013	5:00 AM	1	0
Alert processed after gap	12/27/2013	6:30 AM			1	1
Alert Gap	12/27/2013	8:00 PM	12/27/2013	8:00 PM	1	0
Alert processed after gap	12/27/2013	9:00 PM			2	2

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

Alert Gap	12/28/2013	3:00 PM	12/28/2013	3:00 PM	1	0	(b)(3),6(f),(b)(4)	
Alert processed after gap	12/28/2013	4:00 PM				6		6
Alert Gap	12/28/2013	6:00 PM	12/28/2013	6:00 PM	1	0		
Alert processed after gap	12/28/2013	7:00 PM				58		50
Alert Gap	12/28/2013	10:00 PM	12/28/2013	10:00 PM	1	0		
Alert processed after gap	12/28/2013	11:45 PM				1		1
Alert Gap	12/29/2013	9:00 AM	12/29/2013	9:00 AM	1	0		
Alert processed after gap	12/29/2013	10:00 AM				1		1
Alert Gap	12/29/2013	11:00 AM	12/29/2013	11:00 AM	1	0		
Alert processed after gap	12/29/2013	12:30 PM				2		2
Alert Gap	12/29/2013	4:00 PM	12/29/2013	5:00 PM	2	0		
Alert processed after gap	12/29/2013	6:45 PM				1		1
Alert Gap	12/29/2013	8:00 PM	12/29/2013	8:00 PM	1	0		
Alert processed after gap	12/29/2013	9:30 PM				1		1
Alert Gap	12/29/2013	10:00 PM	12/30/2013	6:00 AM	9	0		
Alert processed after gap	12/30/2013	7:00 AM				2		2
Alert Gap	12/31/2013	6:00 PM	12/31/2013	6:00 PM	1	0		
Alert processed after gap	12/31/2013	7:15 PM				23		23
Alert Gap	12/31/2013	8:00 PM	12/31/2013	8:00 PM	1	0		
Alert processed after gap	12/31/2013	9:00 PM				1		1
Alert Gap	1/1/2014	6:00 AM	1/1/2014	6:00 AM	1	0		
Alert processed after gap	1/1/2014	7:00 AM				1		1
Alert Gap	1/1/2014	8:00 AM	1/1/2014	8:00 AM	1	0		
Alert processed after gap	1/1/2014	9:30 AM				8		8
Alert Gap	1/1/2014	2:00 PM	1/1/2014	2:00 PM	1	0		
Alert processed after gap	1/1/2014	3:15 PM				1		1
Alert Gap	1/1/2014	6:00 PM	1/1/2014	9:00 PM	4	0		
Alert processed after gap	1/1/2014	10:30 PM				1	1	
Alert Gap	1/1/2014	11:00 PM	1/2/2014	12:00 AM	2	0		
Alert processed after gap	1/2/2014	1:00 AM				74	74	
Alert Gap	1/2/2014	2:00 AM	1/2/2014	5:00 AM	4	0		

Alert processed after gap	1/2/2014	6:00 AM			1	1
Alert Gap	1/2/2014	8:00 PM	1/2/2014	8:00 PM	1	0
Alert processed after gap	1/2/2014	9:00 PM			4	4
Alert Gap	1/3/2014	3:00 AM	1/3/2014	3:00 AM	1	0
Alert processed after gap	1/3/2014	4:00 AM			1	1
Alert Gap	1/4/2014	6:00 PM	1/4/2014	6:00 PM	1	0
Alert processed after gap	1/4/2014	7:15 PM			47	42
Alert Gap	1/4/2014	10:00 PM	1/4/2014	11:00 PM	2	0
Alert processed after gap	1/5/2014	12:30 AM			125	116
Alert Gap	1/5/2014	5:00 AM	1/5/2014	5:00 AM	1	0
Alert processed after gap	1/5/2014	6:45 AM			104	95
Alert Gap	1/5/2014	7:00 AM	1/5/2014	9:00 AM	3	0
Alert processed after gap	1/5/2014	10:30 AM			1	1
Alert Gap	1/5/2014	12:00 PM	1/5/2014	12:00 PM	1	0
Alert processed after gap	1/5/2014	1:15 PM			1	1
Alert Gap	1/5/2014	4:00 PM	1/6/2014	5:00 AM	14	0
Alert processed after gap	1/6/2014	6:15 AM			1	1
Alert Gap	1/7/2014	5:00 AM	1/7/2014	5:00 AM	1	0
Alert processed after gap	1/7/2014	6:30 AM			9	9
Alert Gap	1/7/2014	8:00 PM	1/7/2014	8:00 PM	1	0
Alert processed after gap	1/7/2014	9:00 PM			3	3
Alert Gap	1/8/2014	3:00 AM	1/8/2014	3:00 AM	1	0
Alert processed after gap	1/8/2014	4:00 AM			10	10
Alert Gap	1/8/2014	8:00 PM	1/8/2014	8:00 PM	1	0
Alert processed after gap	1/8/2014	9:45 PM			1	1
Alert Gap	1/9/2014	3:00 AM	1/9/2014	3:00 AM	1	0
Alert processed after gap	1/9/2014	4:00 AM			6	6
Alert Gap	1/9/2014	6:00 AM	1/9/2014	6:00 AM	1	0
Alert processed after gap	1/9/2014	7:30 AM			2	2
Alert Gap	1/9/2014	8:00 PM	1/9/2014	8:00 PM	1	0
Alert processed after gap	1/9/2014	9:00 PM			3	3

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

Alert Gap	1/10/2014	5:00 AM	1/10/2014	6:00 AM	2	0	
Alert processed after gap	1/10/2014	7:00 AM				1	1
Alert Gap	1/11/2014	8:00 PM	1/11/2014	8:00 PM	1	0	
Alert processed after gap	1/11/2014	9:00 PM				1	1
Alert Gap	1/11/2014	10:00 PM	1/12/2014	7:00 AM	10	0	
Alert processed after gap	1/12/2014	8:00 AM				204	192
Alert Gap	1/12/2014	12:00 PM	1/12/2014	2:00 PM	3	0	
Alert processed after gap	1/12/2014	3:00 PM				58	50
Alert Gap	1/12/2014	6:00 PM	1/13/2014	3:00 AM	10	0	
Alert processed after gap	1/13/2014	4:00 AM				1	1
Alert Gap	1/13/2014	6:00 AM	1/13/2014	6:00 AM	1	0	
Alert processed after gap	1/13/2014	7:00 AM				1	1
Alert Gap	1/14/2014	9:00 PM	1/14/2014	9:00 PM	1	0	
Alert processed after gap	1/14/2014	10:00 PM				2	2
Alert Gap	1/15/2014	6:00 AM	1/15/2014	6:00 AM	1	0	
Alert processed after gap	1/15/2014	7:00 AM				1	1
Alert Gap	1/15/2014	8:00 PM	1/16/2014	4:00 AM	9	0	
Alert processed after gap	1/16/2014	5:45 AM				304	303
Alert Gap	1/17/2014	3:00 AM	1/17/2014	3:00 AM	1	0	
Alert processed after gap	1/17/2014	4:00 AM				10	10
Alert Gap	1/17/2014	5:00 AM	1/17/2014	5:00 AM	1	0	
Alert processed after gap	1/17/2014	6:00 AM				1	1
Alert Gap	1/17/2014	8:00 PM	1/17/2014	8:00 PM	1	0	
Alert processed after gap	1/17/2014	9:00 PM				1	1
Alert Gap	1/18/2014	8:00 PM	1/18/2014	8:00 PM	1	0	
Alert processed after gap	1/18/2014	9:15 PM				101	79
Alert Gap	1/18/2014	10:00 PM	1/19/2014	12:00 AM	3	0	
Alert processed after gap	1/19/2014	1:45 AM				1	1
Alert Gap	1/19/2014	2:00 AM	1/19/2014	4:00 AM	3	0	
Alert processed after gap	1/19/2014	5:30 AM				3	3
Alert Gap	1/19/2014	10:00 AM	1/19/2014	10:00 AM	1	0	

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

Alert processed after gap	1/19/2014	11:45 AM			1	1
Alert Gap	1/19/2014	12:00 PM	1/19/2014	1:00 PM	2	0
Alert processed after gap	1/19/2014	2:00 PM			1	1
Alert Gap	1/19/2014	5:00 PM	1/19/2014	6:00 PM	2	0
Alert processed after gap	1/19/2014	7:00 PM			1	1
Alert Gap	1/19/2014	9:00 PM	1/19/2014	10:00 PM	2	0
Alert processed after gap	1/19/2014	11:15 PM			1	1
Alert Gap	1/20/2014	12:00 AM	1/20/2014	6:00 AM	7	0
Alert processed after gap	1/20/2014	7:00 AM			11	11
Alert Gap	1/20/2014	3:00 PM	1/20/2014	3:00 PM	1	0
Alert processed after gap	1/20/2014	4:00 PM			1	1
Alert Gap	1/20/2014	6:00 PM	1/20/2014	6:00 PM	1	0
Alert processed after gap	1/20/2014	7:15 PM			2	2
Alert Gap	1/20/2014	10:00 PM	1/20/2014	10:00 PM	1	0
Alert processed after gap	1/20/2014	11:00 PM			1	1
Alert Gap	1/21/2014	12:00 AM	1/21/2014	12:00 AM	1	0
Alert processed after gap	1/21/2014	1:00 AM			64	64
Alert Gap	1/21/2014	2:00 AM	1/21/2014	2:00 AM	1	0
Alert processed after gap	1/21/2014	3:15 AM			6	6
Alert Gap	1/21/2014	4:00 AM	1/21/2014	6:00 AM	3	0
Alert processed after gap	1/21/2014	7:15 AM			1	1
Alert Gap	1/21/2014	8:00 PM	1/22/2014	5:00 AM	10	0
Alert processed after gap	1/22/2014	6:00 AM			432	431
Alert Gap	1/22/2014	8:00 PM	1/22/2014	8:00 PM	1	0
Alert processed after gap	1/22/2014	9:00 PM			6	6
Alert Gap	1/23/2014	6:00 AM	1/23/2014	8:00 AM	3	0
Alert processed after gap	1/23/2014	9:30 AM			20	20
Alert Gap	1/23/2014	8:00 PM	1/23/2014	8:00 PM	1	0
Alert processed after gap	1/23/2014	9:00 PM			2	2
Alert Gap	1/24/2014	5:00 AM	1/24/2014	5:00 AM	1	0
Alert processed after gap	1/24/2014	6:45 AM			1	1

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

Alert Gap	1/25/2014	7:00 PM	1/25/2014	8:00 PM	2	0	
Alert processed after gap	1/25/2014	9:15 PM				25	23
Alert Gap	1/25/2014	10:00 PM	1/25/2014	10:00 PM	1	0	
Alert processed after gap	1/25/2014	11:45 PM				1	1
Alert Gap	1/26/2014	4:00 AM	1/26/2014	5:00 AM	2	0	
Alert processed after gap	1/26/2014	6:30 AM				9	9
Alert Gap	1/26/2014	5:00 PM	1/26/2014	6:00 PM	2	0	
Alert processed after gap	1/26/2014	7:30 PM				2	2
Alert Gap	1/26/2014	9:00 PM	1/27/2013	3:00 AM	7	0	
Alert processed after gap	1/27/2014	4:30 AM				1	1
Alert Gap	1/27/2014	6:00 AM	1/27/2014	6:00 AM	1	0	
Alert processed after gap	1/27/2014	7:00 AM				3	3
Alert Gap	1/27/2014	9:00 PM	1/27/2014	9:00 PM	1	0	
Alert processed after gap	1/27/2014	10:15 PM				37	37
Alert Gap	1/28/2014	5:00 AM	1/28/2014	5:00 AM	1	0	
Alert processed after gap	1/28/2014	6:00 AM				1	1
Alert Gap	1/28/2014	8:00 PM	1/28/2014	8:00 PM	1	0	
Alert processed after gap	1/28/2014	9:00 PM				1	1
Alert Gap	1/28/2014	10:00 PM	1/29/2014	5:00 AM	8	0	
Alert processed after gap	1/29/2014	6:45 AM				32	32
Alert Gap	1/29/2014	8:00 AM	1/29/2014	8:00 AM	1	0	
Alert processed after gap	1/29/2014	9:00 AM				2	2
Alert Gap	1/30/2014	8:00 PM	1/30/2014	8:00 PM	1	0	
Alert processed after gap	1/30/2014	9:00 PM				3	3
Alert Gap	1/30/2014	11:00 PM	1/31/2014	5:00 AM	7	0	
Alert processed after gap	1/31/2014	6:45 AM				55	55
Alert Gap	1/31/2014	8:00 PM	1/31/2014	8:00 PM	1	0	
Alert processed after gap	1/31/2014	9:15 PM				4	4
Alert Gap	1/31/2014	10:00 PM	2/1/2014	6:00 AM	9	0	
Alert processed after gap	2/1/2014	7:30 AM				539	521
Alert Gap	2/1/2014	10:00 PM	2/1/2014	2:00 PM	5	0	

(b)(3);6(f);(b)(4)

Alert processed after gap	2/2/2014	3:15 AM			260	230
Alert Gap	2/2/2014	8:00 AM	2/2/2014	10:00 AM	3	0
Alert processed after gap	2/2/2014	11:00 AM			58	55
Alert Gap	2/2/2014	12:00 PM	2/2/2014	2:00 PM	3	0
Alert processed after gap	2/2/2014	3:00 PM			45	45
Alert Gap	2/2/2014	4:00 PM	2/2/2014	5:00 PM	2	0
Alert processed after gap	2/2/2014	6:30 PM			1	1
Alert Gap	2/2/2014	8:00 PM	2/2/2014	8:00 PM	1	0
Alert processed after gap	2/2/2014	9:00 PM			1	1
Alert Gap	2/2/2014	10:00 PM	2/3/2014	4:00 AM	7	0
Alert processed after gap	2/3/2014	5:15 AM			1	1
Alert Gap	2/4/2014	12:00 AM	2/4/2014	6:00 AM	7	0
Alert processed after gap	2/4/2014	7:00 AM			306	306
Alert Gap	2/4/2014	8:00 PM	2/4/2014	8:00 PM	1	0
Alert processed after gap	2/4/2014	9:00 PM			2	2
Alert Gap	2/5/2014	3:00 AM	2/5/2014	3:00 AM	1	0
Alert processed after gap	2/5/2014	4:00 AM			9	9
Alert Gap	2/5/2014	5:00 AM	2/5/2014	5:00 AM	1	0
Alert processed after gap	2/5/2014	6:00 AM			2	2
Alert Gap	2/5/2014	8:00 PM	2/5/2014	8:00 PM	1	0
Alert processed after gap	2/5/2014	9:00 PM			1	1
Alert Gap	2/6/2014	5:00 AM	2/6/2014	5:00 AM	1	0
Alert processed after gap	2/6/2014	6:15 AM			1	1
Alert Gap	2/6/2014	8:00 PM	2/6/2014	8:00 PM	1	0
Alert processed after gap	2/6/2014	9:00 PM			1	1
Alert Gap	2/7/2014	3:00 AM	2/7/2014	3:00 AM	1	0
Alert processed after gap	2/7/2014	4:00 AM			9	9
Alert Gap	2/7/2014	6:00 AM	2/7/2014	6:00 AM	1	0
Alert processed after gap	2/7/2014	7:00 AM			1	1
Alert Gap	2/8/2014	7:00 PM	2/8/2014	7:00 PM	1	0
Alert processed after gap	2/8/2014	8:45 PM			101	89

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

Alert Gap	2/8/2014	10:00 PM	2/8/2014	10:00 PM	1	0	
Alert processed after gap	2/8/2014	11:45 PM				1	1
Alert Gap	2/9/2014	5:00 AM	2/9/2014	5:00 AM	1	0	
Alert processed after gap	2/9/2014	6:45 AM				102	91
Alert Gap	2/9/2014	7:00 AM	2/9/2014	8:00 AM	2	0	
Alert processed after gap	2/9/2014	9:15 AM				1	1
Alert Gap	2/9/2014	11:00 AM	2/9/2014	12:00 PM	2	0	
Alert processed after gap	2/9/2014	1:45 PM				1	1
Alert Gap	2/9/2014	3:00 PM	2/9/2014	3:00 PM	1	0	
Alert processed after gap	2/9/2014	4:00 PM				1	1
Alert Gap	2/9/2014	5:00 PM	2/9/2014	5:00 PM	1	0	
Alert processed after gap	2/9/2014	6:45 PM				1	1
Alert Gap	2/9/2014	7:00 PM	2/10/2014	4:00 AM	10	0	
Alert processed after gap	2/10/2014	5:45 AM				2	2
Alert Gap	2/10/2014	6:00 AM	2/10/2014	6:00 AM	1	0	
Alert processed after gap	2/10/2014	7:00 AM				3	3
Alert Gap	2/11/2014	9:00 PM	2/12/2014	6:00 AM	10	0	
Alert processed after gap	2/12/2014	7:00 AM				78	78
Alert Gap	2/12/2014	8:00 PM	2/12/2014	8:00 PM	1	0	
Alert processed after gap	2/12/2014	9:00 PM				1	1
Alert Gap	2/12/2014	11:00 PM	2/13/2014	5:00 AM	7	0	
Alert processed after gap	2/13/2014	6:15 AM				129	129
Alert Gap	2/13/2014	8:00 AM	2/13/2014	8:00 AM	1	0	
Alert processed after gap	2/13/2014	9:00 AM				5	5
Alert Gap	2/13/2014	9:00 PM	2/14/2014	6:00 AM	10	0	
Alert processed after gap	2/14/2014	7:15 AM				30	30
Alert Gap	2/14/2014	8:00 PM	2/14/2014	8:00 PM	1	0	
Alert processed after gap	2/14/2014	9:00 PM				2	2
Alert Gap	2/14/2014	10:00 PM	2/15/2014	12:00 AM	3	0	
Alert processed after gap	2/15/2014	1:00 AM				250	250
Alert Gap	2/15/2014	3:00 PM	2/15/2014	3:00 PM	1	0	

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

Alert processed after gap	2/15/2014	4:00 PM			1	1
Alert Gap	2/15/2014	7:00 PM	2/15/2014	7:00 PM	1	0
Alert processed after gap	2/15/2014	8:45 PM			106	97
Alert Gap	2/16/2014	4:00 AM	2/16/2014	5:00 AM	2	0
Alert processed after gap	2/16/2014	6:15 AM			2	2
Alert Gap	2/16/2014	2:00 PM	2/16/2014	2:00 PM	1	0
Alert processed after gap	2/16/2014	3:00 PM			1	1
Alert Gap	2/16/2014	8:00 PM	2/17/2014	6:00 AM	11	0
Alert processed after gap	2/17/2014	7:00 AM			3	3
Alert Gap	2/17/2014	4:00 PM	2/17/2014	4:00 PM	1	0
Alert processed after gap	2/17/2014	5:15 PM			2	2
Alert Gap	2/17/2014	9:00 PM	2/17/2014	11:00 PM	3	0
Alert processed after gap	2/18/2014	12:00 AM			16	16
Alert Gap	2/18/2014	1:00 AM	2/18/2014	2:00 AM	2	0
Alert processed after gap	2/18/2014	3:30 AM			7	7
Alert Gap	2/18/2014	5:00 AM	2/18/2014	6:00 AM	2	0
Alert processed after gap	2/18/2014	7:00 AM			1	1
Alert Gap	2/18/2014	8:00 PM	2/18/2014	8:00 PM	1	0
Alert processed after gap	2/18/2014	9:00 PM			3	3
Alert Gap	2/19/2014	8:00 PM	2/19/2014	8:00 PM	1	0
Alert processed after gap	2/19/2014	9:00 PM			1	1
Alert Gap	2/20/2014	5:00 AM	2/20/2014	5:00 AM	1	0
Alert processed after gap	2/20/2014	6:15 AM			1	1
Alert Gap	2/21/2014	5:00 AM	2/21/2014	5:00 AM	1	0
Alert processed after gap	2/21/2014	6:00 AM			1	1
Alert Gap	2/21/2014	8:00 PM	2/21/2014	8:00 PM	1	0
Alert processed after gap	2/21/2014	9:00 PM			2	2
Alert Gap	2/22/2014	4:00 PM	2/22/2014	4:00 PM	1	0
Alert processed after gap	2/22/2014	5:30 PM			14	14
Alert Gap	2/22/2014	8:00 PM	2/22/2014	8:00 PM	1	0
Alert processed after gap	2/22/2014	9:00 PM			3	3

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

Alert Gap	2/22/2014	10:00 PM	2/22/2014	10:00 PM	1	0	
Alert processed after gap	2/22/2014	11:15 PM				1	1
Alert Gap	2/23/2014	5:00 AM	2/23/2014	6:00 AM	2	0	
Alert processed after gap	2/23/2014	7:00 AM				91	81
Alert Gap	2/23/2014	8:00 AM	2/23/2014	11:00 AM	4	0	
Alert processed after gap	2/23/2014	12:00 PM				1	1
Alert Gap	2/23/2014	1:00 PM	2/23/2014	1:00 PM	1	0	
Alert processed after gap	2/23/2014	2:15 PM				1	1
Alert Gap	2/23/2014	5:00 PM	2/24/2014	3:00 AM	11	0	
Alert processed after gap	2/24/2014	4:00 AM				1	1
Alert Gap	2/24/2014	5:00 AM	2/24/2014	5:00 AM	1	0	
Alert processed after gap	2/24/2014	6:00 AM				1	1
Alert Gap	2/24/2014	8:00 PM	2/24/2014	8:00 PM	1	0	
Alert processed after gap	2/24/2014	9:00 PM				5	5
Alert Gap	2/25/2014	2:00 AM	2/25/2014	2:00 AM	1	0	
Alert processed after gap	2/25/2014	3:00 AM				10	10
Alert Gap	2/25/2014	5:00 AM	2/25/2014	5:00 AM	1	0	
Alert processed after gap	2/25/2014	6:30 AM				3	3
Alert Gap	2/25/2014	8:00 PM	2/26/2014	5:00 AM	10	0	
Alert processed after gap	2/26/2014	6:30 AM				269	269
Alert Gap	2/26/2014	8:00 PM	2/26/2014	8:00 PM	1	0	
Alert processed after gap	2/26/2014	9:00 PM				2	2
Alert Gap	2/27/2014	8:00 PM	2/28/2014	5:00 AM	10	0	
Alert processed after gap	2/28/2014	6:30 AM				332	331
Alert Gap	2/28/2014	11:00 PM	3/1/2014	12:00 AM	2	0	
Alert processed after gap	3/1/2014	1:45 AM				301	301
Alert Gap	3/1/2014	11:00 PM	3/1/2014	11:00 PM	1	0	
Alert processed after gap	3/2/2014	12:30 AM				124	104
Alert Gap	3/2/2014	4:00 AM	3/2/2014	4:00 AM	1	0	
Alert processed after gap	3/2/2014	5:00 AM				1	1
Alert Gap	3/2/2014	2:00 PM	3/2/2014	3:00 PM	2	0	

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

Alert processed after gap	3/2/2014	4:45 PM			2	2
Alert Gap	3/2/2014	6:00 PM	3/2/2014	9:00 PM	4	0
Alert processed after gap	3/2/2014	10:00 PM			1	1
Alert Gap	3/2/2014	11:00 PM	3/3/2014	12:00 AM	2	0
Alert processed after gap	3/3/2014	1:45 AM			1	1
Alert Gap	3/3/2014	2:00 AM	3/3/2014	5:00 AM	4	0
Alert processed after gap	3/3/2014	6:00 AM			1	1
Alert Gap	3/4/2014	9:00 PM	3/5/2014	5:00 AM	9	0
Alert processed after gap	3/5/2014	6:30 AM			22	22
Alert Gap	3/6/2014	3:00 AM	3/6/2014	3:00 AM	1	0
Alert processed after gap	3/6/2014	4:00 AM			3	3
Alert Gap	3/6/2014	5:00 AM	3/6/2014	5:00 AM	1	0
Alert processed after gap	3/6/2014	6:00 AM			2	2
Alert Gap	3/6/2014	8:00 PM	3/7/2014	5:00 AM	10	0
Alert processed after gap	3/7/2014	6:30 AM			307	307
Alert Gap	3/7/2014	8:00 PM	3/7/2014	8:00 PM	1	0
Alert processed after gap	3/7/2014	9:00 PM			1	1
Alert Gap	3/8/2014	7:00 PM	3/8/2014	7:00 PM	1	0
Alert processed after gap	3/8/2014	8:00 PM			125	106
Alert Gap	3/9/2014	7:00 AM	3/9/2014	10:00 AM	4	0
Alert processed after gap	3/9/2014	11:00 AM			1	1
Alert Gap	3/9/2014	4:00 PM	3/9/2014	4:00 PM	1	0
Alert processed after gap	3/9/2014	5:00 PM			91	86
Alert Gap	3/9/2014	7:00 PM	3/9/2014	11:00 PM	5	0
Alert processed after gap	3/10/2014	12:30 AM			1	1
Alert Gap	3/10/2014	2:00 AM	3/10/2014	3:00 AM	2	0
Alert processed after gap	3/10/2014	4:30 AM			1	1
Alert Gap	3/10/2014	5:00 AM	3/10/2014	5:00 AM	1	0
Alert processed after gap	3/10/2014	6:00 AM			4	4
Alert Gap	3/10/2014	7:00 PM	3/10/2014	7:00 PM	1	0
Alert processed after gap	3/10/2014	8:00 PM			4	4

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

Alert Gap	3/11/2014	4:00 AM	3/11/2014	4:00 AM	1	0	(b)(3);6(f),(b)(4)	
Alert processed after gap	3/11/2014	5:45 AM				9		9
Alert Gap	3/12/2014	4:00 AM	3/12/2014	4:00 AM	1	0		
Alert processed after gap	3/12/2014	5:00 AM				2		2
Alert Gap	3/12/2014	8:00 PM	3/12/2014	8:00 PM	1	0		
Alert processed after gap	3/12/2014	9:00 PM				35		35
Alert Gap	3/13/2014	5:00 AM	3/13/2014	5:00 AM	1	0		
Alert processed after gap	3/13/2014	6:00 AM				2		2
Alert Gap	3/13/2014	9:00 PM	3/14/2014	4:00 AM	8	0		
Alert processed after gap	3/14/2014	5:30 AM				291		291

* Planned and Unplanned maintenance accounts for some portion of the gap; unable to determine the cause for the remaining time period

** Initial review of data indicates potential planned/ unplanned outage however we are unable to definitively determine

EXHIBIT B

EWS Alerts - List of Weekends where alerts were not processed

Label	Start Date	Start Time	End Date	End Time	Potential Duration (in hrs)	# of Alerts Processed	# of Members Impacted	Notes	GAP_START MEM_COUNT	GAP_END MEM_COUNT
Alert Gap	10/12/2012	7:00 PM	10/15/2012	7:00 AM	61	0		Weekend alerts not processed	1677491	1680288
Alert processed after gap	10/15/2012	8:00 AM				502	464			
Alert Gap	11/2/2012	6:00 PM	11/5/2012	7:00 AM	62	0		Weekend alerts not processed	1723296	1726202
Alert processed after gap	11/5/2012	8:00 AM				363	328			
Alert Gap	11/9/2012	6:00 AM	11/12/2012	7:00 AM	62	0		Weekend alerts not processed	1734657	1738692
Alert processed after gap	11/12/2012	8:00 AM				165	158			
Alert Gap	11/16/2012	5:00 PM	11/19/2012	7:00 AM	63	0		Weekend alerts not processed	1748272	1750936
Alert processed after gap	11/19/2012	8:00 AM				506	475			
Alert Gap	11/23/2012	5:00 PM	11/26/2012	7:00 AM	63	0		Weekend alerts not processed	1760500	1763303
Alert processed after gap	11/26/2012	8:00 AM				234	220			
Alert Gap	11/30/2012	6:00 PM	12/3/2012	7:00 AM	62	0		Weekend alerts not processed	1774594	1777313
Alert processed after gap	12/3/2012	8:00 AM				315	291			
Alert Gap	12/7/2012	6:00 PM	12/10/2012	8:00 AM	63	0		Weekend alerts not processed	1786457	1788806
Alert processed after gap	12/10/2012	9:15 AM				444	426			
Alert Gap	12/14/2012	6:00 PM	12/17/2012	7:00 AM	62	0		Weekend alerts not processed	1797063	1799176
Alert processed after gap	12/17/2012	8:00 AM				353	347			
Alert Gap	12/21/2012	5:00 PM	12/24/2012	7:00 AM	63	0		Weekend alerts not processed	1808945	1811310
Alert processed after gap	12/24/2012	8:00 AM				302	265			
Alert Gap	12/28/2012	6:00 PM	12/31/2012	7:00 AM	62	0		Weekend alerts not processed	1818268	1820818
Alert processed after gap	12/31/2012	8:00 AM				371	331			
Alert Gap	1/4/2013	6:00 PM	1/7/2013	7:00 AM	62	0		Weekend alerts not processed	1829782	1832526
Alert processed after gap	1/7/2013	8:00 AM				425	384			
Alert Gap	1/11/2013	6:00 PM	1/14/2013	7:00 AM	62	0		Weekend alerts not processed	1843130	1846162
Alert processed after gap	1/14/2013	8:00 AM				343	319			
Alert Gap	1/18/2013	6:00 PM	1/21/2013	7:00 AM	62	0		Weekend alerts not processed	1857584	1860410
Alert processed after gap	1/21/2013	8:00 AM				374	334			
Alert Gap	1/25/2013	5:00 PM	1/28/2013	7:00 AM	63	0		Weekend alerts not processed	1870871	1874266
Alert processed after gap	1/28/2013	8:00 AM				88	86			
Alert Gap	2/1/2013	6:00 PM	2/4/2013	7:00 AM	62	0		Weekend alerts not processed	1885519	1888621
Alert processed after gap	2/4/2013	8:00 AM				439	411			
Alert Gap	2/8/2013	6:00 PM	2/11/2013	7:00 AM	62	0		Weekend alerts not processed	1901233	1904828
Alert processed after gap	2/11/2013	8:00 AM				522	473			

Alert Gap	2/15/2013	6:00 PM	2/18/2013	7:00 AM	62	0	Weekend alerts not processed (incl	1916500	1920187
Alert processed after gap	2/18/2013	8:00 AM				512	475		
Alert Gap	2/22/2013	6:00 PM	2/25/2013	7:00 AM	62	0	Weekend alerts not processed	1932006	1935772
Alert processed after gap	2/25/2013	8:00 AM				355	299		
Alert Gap	3/1/2013	6:00 PM	3/4/2013	7:00 AM	62	0	Weekend alerts not processed	1949299	1954295
Alert processed after gap	3/4/2013	8:00 AM				167	157		
Alert Gap	3/8/2013	6:00 PM	3/11/2013	7:00 AM	62	0	Weekend alerts not processed	1969175	1973350
Alert processed after gap	3/11/2013	8:00 AM				166	149		
Alert Gap	3/15/2013	6:00 PM	3/18/2013	6:00 AM	61	0	Weekend alerts not processed	1986366	1990428
Alert processed after gap	3/18/2013	7:45 AM				85	80		
Alert Gap	3/22/2013	6:00 PM	3/25/2013	7:00 AM	62	0	Weekend alerts not processed	2003197	2006815
Alert processed after gap	3/25/2013	8:00 AM				480	455		
Alert Gap	3/29/2013	6:00 PM	4/1/2013	7:00 AM	62	0	Weekend alerts not processed	2019029	2022357
Alert processed after gap	4/1/2013	8:00 AM				377	356		
Alert Gap	4/5/2013	6:00 PM	4/8/2013	7:00 AM	62	0	Weekend alert not processed	2034354	2037405
Alert processed after gap	4/8/2013	8:00 AM				467	450		
Alert Gap	4/12/2013	6:00 PM	4/15/2013	7:00 AM	62	0	Weekend alerts not processed	2051285	2055931
Alert processed after gap	4/15/2013	8:00 AM				226	216		
Alert Gap	4/19/2013	6:00 PM	4/22/2013	7:00 AM	62	0	Weekend alerts not processed	2068659	2072342
Alert processed after gap	4/22/2013	8:00 AM				96	94		
Alert Gap	4/26/2013	5:00 PM	4/29/2013	7:00 AM	63	0	Weekend alerts not processed	2084302	2088039
Alert processed after gap	4/29/2013	8:00 AM				427	410		
Alert Gap	5/3/2013	6:00 PM	5/6/2013	7:00 AM	62	0	Weekend alerts not processed	2100119	2103598
Alert processed after gap	5/6/2013	8:00 AM				365	338		
Alert Gap	5/10/2013	6:00 PM	5/13/2013	7:00 AM	62	0	Weekend alerts not processed	2115609	2118594
Alert processed after gap	5/13/2013	8:00 AM				423	403		
Alert Gap	5/17/2013	6:00 PM	5/20/2013	7:00 AM	62	0	Weekend alerts not processed	2129628	2133121
Alert processed after gap	5/20/2013	8:00 AM				326	292		
Alert Gap	5/24/2013	6:00 PM	5/28/2013	7:00 AM	86	0	Weekend alerts not processed	2143911	2148433
Alert processed after gap	5/28/2013	8:00 AM				383	373		
Alert Gap	5/31/2013	6:00 PM	6/3/2013	7:00 AM	62	0	Weekend alerts not processed	2156924	2161250
Alert processed after gap	6/3/2013	8:00 AM				341	314		
Alert Gap	6/7/2013	6:00 PM	6/10/2013	7:00 AM	62	0	Weekend alerts not processed	2172559	2175909
Alert processed after gap	6/10/2013	8:00 AM				252	216		
Alert Gap	6/14/2013	6:00 PM	6/17/2013	7:00 AM	62	0	Weekend alerts not processed	2186846	2189828
Alert processed after gap	6/17/2013	8:30 AM				22	22		
Alert Gap	6/21/2013	5:00 PM	6/24/2013	7:00 AM	63	0	Weekend alerts not processed	2201141	2204379

Alert processed after gap	6/24/2013	8:00 AM			340	328			
Alert Gap	6/27/2013	5:00 PM	7/1/2013	8:00 AM	88	0	Weekend alerts not processed (Incl	2212897	2219179
Alert processed after gap	7/1/2013	9:30 AM			31	29			
Alert Gap	7/5/2013	5:00 PM	7/8/2013	6:00 AM	63	0	Weekend alerts not processed	2228705	2231967
Alert processed after gap	7/8/2013	8:00 AM			285	269			
Alert Gap	7/19/2013	6:00 PM	7/23/2013	7:00 AM	86	0	Weekend alerts not processed	2257416	2262983
Alert processed after gap	7/23/2013	8:00 AM			558	499			
Alert Gap	8/2/2013	7:00 PM	8/5/2013	9:00 AM	63	0	Weekend alerts not processed	2287211	2290802
Alert processed after gap	8/5/2013	10:45 AM			308	306			
Alert Gap	11/1/2013	7:00 PM	11/4/2013	8:00 AM	62	0	Weekend alerts not processed	2501493	2505851
Alert processed after gap	11/4/2013	9:45 AM			209	198			
Alert Gap	11/8/2013	7:00 PM	11/12/2013	6:00 AM	84	0	Weekend alerts not processed (Incl	2518875	2524572
Alert processed after gap	11/13/2013	7:15 AM			74	74			
Alert Gap	11/24/2013	8:00 AM	11/27/2013	8:00 AM	73	0	Partial Weekend (Includes Planned	2554739	2562169
Alert processed after gap	11/27/2013	9:00 AM			195	187			

EXHIBIT C

Number of Gaps in Alerts by Duration and Expectation

	Planned	Unplanned or other	Total
5-9 hours	78	75	153
10-59 hours	59	33	92
60+ hours	4	38	42
Any duration	155	1,103	1,258

EXHIBIT D

Timespan of VRR Data

	Oldest	Newest
Created Time	6-Apr-12	7-May-15
Date of Note	12-Apr-12	27-May-15
Completed Time	18-May-12	18-May-15

EXHIBIT E

Number of Tickets by Criticality and Request Status

Request Status	Critical	High	Medium	Low	Not stated	Total
Closed	210	245	331	685	253	1,724
On Hold	0	2	0	0	2	4
Open	10	48	40	23	92	213
Total	220	295	371	708	347	1,941

EXHIBIT F

Average Days from Vulnerability Discovery to Ticket Completed Date by Criticality and by Ticket Creation Date Calendar Quarter

Criticality	Discovery to ticket creation	Discovery to first note	Discovery to resolution	Discovery to completion	Ticket creation to first note	Ticket creation to resolution	Ticket creation to completion
Critical	43	70	148	209	27	107	166
High	43	116	125	252	72	82	208
Medium	28	67	111	184	39	88	159
Low	24	94	122	206	68	101	182
Not stated	25	75	115	189	49	97	168
Total	30	86	122	206	55	96	177

Ticket Creation Quarter	Discovery to ticket creation	Discovery to first note	Discovery to resolution	Discovery to completion	Ticket creation to first note	Ticket creation to resolution	Ticket creation to completion
2012 Q2	8	98	118	169	84	113	165
2012 Q3	12	91	120	163	80	108	151
2012 Q4	20	121	162	315	101	141	295
2013 Q1	22	65	108	189	45	87	172
2013 Q2	48	116	148	244	68	99	197
2013 Q3	78	145	150	283	66	75	204
2013 Q4	49	79	148	234	32	95	187
2014 Q1	16	40	92	171	30	78	156
2014 Q2	33	41	131	189	18	92	185
2014 Q3	30	66	106	301	34	73	268
2014 Q4	6	36	76	207	31	71	190
2015 Q1	42	53	89	126	12	51	85
2015 Q2	12	38	8	48	19	4	35
Total	30	86	122	206	55	96	177

EXHIBIT G

Tickets with Vulnerability Discovery to First Date of Note greater than 30 Days, 60 Days, and 90 Days by Criticality and by Ticket Creation Date Calendar Quarter

Criticality	Discovery to first note greater than 30 days	Discovery to first note greater than 60 days	Discovery to first note greater than 90 days	Indeterminable ¹	Total number of tickets
Critical	147	69	47	28	220
High	162	148	107	75	295
Medium	190	119	73	94	371
Low	410	280	221	200	708
Not stated	153	106	51	139	347
Total	1,062	722	499	536	1,941

Ticket Creation Quarter	Discovery to first note greater than 30 days	Discovery to first note greater than 60 days	Discovery to first note greater than 90 days	Indeterminable ¹	Total number of tickets
2012 Q2	85	60	38	132	242
2012 Q3	74	73	47	66	213
2012 Q4	126	116	91	45	178
2013 Q1	110	41	24	44	170
2013 Q2	169	127	98	16	185
2013 Q3	142	142	125	12	156
2013 Q4	177	57	50	29	206
2014 Q1	45	41	13	64	292
2014 Q2	21	10	1	25	53
2014 Q3	23	14	5	4	32
2014 Q4	10	3	2	12	30
2015 Q1	70	36	5	74	160
2015 Q2	10	2	0	13	24
Total	1,062	722	499	536	1,941

¹ Indeterminable because no date was included in either the “Description” field or the “Date of Note” field.

EXHIBIT H

Tickets with Vulnerability Discovery to Resolution Date greater than 30 Days, 60 Days, and 90 Days by Criticality and by Ticket Creation Date Calendar Quarter

Criticality	Discovery to resolution date greater than 30 days	Discovery to resolution date greater than 60 days	Discovery to resolution date greater than 90 days	Indeterminable ¹	Total number of tickets
Critical	133	132	80	85	220
High	153	152	109	141	295
Medium	250	247	112	121	371
Low	516	448	288	192	708
Not stated	176	159	74	167	347
Total	1,228	1,138	663	706	1,941

Ticket Creation Quarter	Discovery to resolution date greater than 30 days	Discovery to resolution date greater than 60 days	Discovery to resolution date greater than 90 days	Indeterminable ¹	Total number of tickets
2012 Q2	189	173	73	50	242
2012 Q3	186	183	50	27	213
2012 Q4	84	78	74	94	178
2013 Q1	150	89	83	20	170
2013 Q2	119	119	119	66	185
2013 Q3	94	91	90	62	156
2013 Q4	97	97	53	109	206
2014 Q1	243	243	77	49	292
2014 Q2	32	32	32	21	53
2014 Q3	1	1	1	30	32
2014 Q4	3	2	2	27	30
2015 Q1	30	30	9	129	160
2015 Q2	0	0	0	22	24
Total	1,228	1,138	663	706	1,941

¹ Indeterminable because no date was included in either the “Description” field or the “Resolution” field.

EXHIBIT I

Tickets with Critical or High Criticality

Ticket Created Date	Critical	High
September 1, 2012 through February 21, 2013	0	1
March 13, 2013 through June 25, 2013	0	1