ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 of 3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 09/16/2013	2. CONTRACT NO. (If any): D13PC00025
3. ORDER NO.: D13PD01512	4. REQUISITION/REFERENCE NO.:
5. ISSUING OFFICE (Address correspondence to): Interior Business Center, AQD Division 2 /Branch 3 381 Elden St Suite 4000 Herndon VA 20170	6. SHIP TO: a. NAME OF CONSIGNEE: See Attached Schedule b. STREET ADDRESS: See Attached Schedule c. CITY: See Attached Schedule d. STATE: CO e. ZIP CODE: 80235
7. TO: ATTN GOVERNMENT POC a. NAME OF CONTRACTOR: UNISYS CORPORATION b. COMPANY NAME: c. STREET ADDRESS: 11720 PLAZA AMERICA DR TOWER III d. CITY: RESTON e. STATE: VA f. ZIP CODE: 20190-4757	f. SHIP VIA: 8. TYPE OF ORDER ☐ a. PURCHASE REFERENCE YOUR: Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated. ☒ b. DELIVERY Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.
9. ACCOUNTING AND APPROPRIATION DATA: See Schedule	10. REQUISITIONING OFFICE: DOI ACQ SVCS DIRECTORATE
11. BUSINESS CLASSIFICATION (Check appropriate box(es)): ☐ a. SMALL ☒ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone ☐ f. SERVICE-DISABLED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB	12. F.O.B. POINT: Destination
13. PLACE OF a. INSPECTION: Destination b. ACCEPTANCE: Destination	14. GOVERNMENT B/L NO.:
15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date): 09/15/2014	16. DISCOUNT TERMS: ACCP

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The contractor's quote, dated 8/29/13, is hereby incorporated into this task order by reference with the same force and effect as if included in full text. Any conflict between the terms and conditions of this task order and the contractor's quote, Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO:			
a. NAME: Invoice Processing Platform System			$139,675.74
SEE BILLING INSTRUCTIONS ON REVERSE b. STREET ADDRESS (or P.O. Box): US Department of Treasury http://www.ipp.gov			17(i) GRAND TOTAL
c. CITY	d. STATE	e. ZIP CODE	$139,675.74

22. UNITED STATES OF AMERICA BY (Signature):

23. NAME (Typed): Rob Stoltz
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/16/2013	D13PC00025	D13PD01512

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	shall be resolved by giving precedence to the terms and conditions contained in this task order. This task order is being issued as a Time & Materials (T&M) type award. The total overall value of this task order is $463,436.75 (base and all option periods, if exercised). Admin Office: DOI, Interior Business Center, AQD Division 2/Branch 3 381 Elden St Suite 4000 Herndon VA 20170 Accounting Info: Period of Performance: 09/16/2013 to 09/15/2014					
00010	FHFA IaaS - Public Facing Website It is estimated that the total cost to the Government for full performance of the base period will be a Not-To-Exceed (NTE) amount of $139,436.75. Total funds currently available and allotted to this task order are $139,436.75 which fully funds the base period. The Government shall not be obligated to reimburse the Contractor for costs in excess of the current allotment, nor will the Contractor be obligated to continue performance and incur costs in excess of the amount allotted. All terms and conditions applicable to IDIQ Contract No. D13PC00025 are applicable to this task order and any/all subsequent modifications unless otherwise agreed upon. Continued ...				139,675.74	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $139,675.74

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/16/2013	D13PC00025	D13PD01512

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The total amount of award: $139,675.74. The obligation for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) > $0.00

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 19

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 05/01/2013	2. CONTRACT NO. (If any): D13PC00025
3. ORDER NO.: D13PD00827	4. REQUISITION/REFERENCE NO.: 0040087097

5. ISSUING OFFICE (Address correspondence to):
Interior Business Center, AQD
Division 2 /Branch 3
381 Elden St
Suite 4000
Herndon VA 20170

6. SHIP TO:
a. NAME OF CONSIGNEE: FBMS PMO
b. STREET ADDRESS: 13461 Sunrise Valley Drive, Suite 1
c. CITY: Herndon | d. STATE: VA | e. ZIP CODE: 20171

7. TO: ATTN GOVERNMENT POC
a. NAME OF CONTRACTOR: UNISYS CORPORATION
b. COMPANY NAME:
c. STREET ADDRESS: 11720 PLAZA AMERICA DR TOWER III
d. CITY: RESTON | e. STATE: VA | f. ZIP CODE: 20190-4757

f. SHIP VIA:

8. TYPE OF ORDER
☐ a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Schedule

10. REQUISITIONING OFFICE: DOI ACQ SVCS DIRECTORATE

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☐ a. SMALL ☒ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT: Destination

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE			
Destination	Destination		04/30/2015	ACCP

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Admin Office: DOI, Interior Business Center, AQD Division 2/Branch 3 381 Elden St Suite 4000 Herndon VA 20170 Continued ...					

18. SHIPPING POINT
19. GROSS SHIPPING WEIGHT
20. INVOICE NO.
17(h) TOTAL (Cont. pages)

21. MAIL INVOICE TO:
a. NAME: Invoice Processing Platform System
$2,298,990.00

SEE BILLING INSTRUCTIONS ON REVERSE
b. STREET ADDRESS (or P.O. Box): US Department of Treasury
http://www.ipp.gov
17(i) GRAND TOTAL
$2,298,990.00

c. CITY | d. STATE | e. ZIP CODE

22. UNITED STATES OF AMERICA BY (Signature): Terrie L Callahan

23. NAME (Typed): Terrie Callahan
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER	CONTRACT NO.	ORDER NO.
05/01/2013	D13PC00025	D13PD00827

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Accounting Info: Period of Performance: 05/01/2013 to 04/30/2015 The SAP Application Hosting Pilot Phase period of performance is from May 1, 2013 through September 30, 2013. Current funding allocated to this task order is for Pilot Phase only. Additional funding for architecture & planning and migration may be provided via modification prior to completion of pilot. This task order is being issued as a Time & Materials (T&M) type award.					
00010	SAP Application Hosting Pilot Phase				2,298,990.00	
	The total amount of award: $2,298,990.00. The obligation for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $2,298,990.00

SAP Application Hosting of the Department of the Interior's Financial and Business Management System (FBMS)

1. BACKGROUND

1.1. FBMS integrates and streamlines the Department of the Interior's (DOI) financial and administrative functions across all DOI Bureaus. Before FBMS, the lack of integration among DOI systems burdened resources and hindered real-time business decision making. Implementing FBMS supports the Department in incorporating its financial and business management processes into a single solution that eliminates the need for more than 80 DOI and bureau specific systems currently in operation.

1.2. DOI has adopted a phased approach to deploying FBMS across its Bureaus. To date, the Office of Surface Mining (OSM), the Bureau of Ocean Energy Management, (BOEM), the Bureau of Safety and Environmental Enforcement (BSEE), the Bureau of Land Management (BLM), the U.S. Geological Survey (USGS), the U. S. Fish and Wildlife Service (FWS), National Park Service (NPS), Indian Affairs (IA), and the organizations within the Departmental Office (DO) have deployed FBMS. These Bureaus are using FBMS functionality to perform operations related to core financials, acquisitions, personal property, fleet management, financial assistance, and travel management.

1.3. The Bureau of Reclamation (BOR) is scheduled to deploy FBMS as part of Deployment 8 (D8) in November 2013.

1.4. The FBMS will be the sole fiscal accounting system for the Department's annual budget and is the central enterprise management system in support of all of the Department's mission programs.

1.5. Currently, the FBMS infrastructure is hosted by the DOI's National Business Center (NBC) at two locations. The Development, Test, and Disaster Recovery environments reside in the NBC's Eastern Service Center in Reston, VA, while the Production, Production Mirror (ProdCopy), and Training environments are maintained in the NBC's Denver Data Center, in Denver, CO. The FBMS Program Management Office (PMO) also maintains office locations in Herndon, VA and in the Denver Federal Center in Lakewood, CO. Consistent with the federal government's 25-point IT Transformation initiative, Federal Cloud Computing Strategy, and Cloud-First policy, the FBMS PMO intends to transition its data center based hosting to a cloud-based infrastructure service. DOI shall retain the ability to perform the same capabilities for ProdCopy and backups via the next technical platform in the cloud.

2. SCOPE

2.1. The scope of this Task Order is the provision of an infrastructure type service offering for hosting FBMS that:

- Supports the system's needs in terms of processing power, memory, storage, and connectivity;

- Operates within the enumerated constraints; and
- Meets or exceeds the acceptable quality levels and performance standards

2.2. The scope includes assessment of the current FBMS infrastructure and operations, transition planning, implementation management, and operations management/optimization of the provided infrastructure services.

3. CURRENT ENVIRONMENT AND REQUIREMENT PROJECTIONS

3.1. The DOI has standardized on an Enterprise Resource Planning (ERP) application based upon SAP. This standard ERP, customized for use by the Bureaus in the DOI, is known as the FBMS. At the time of migration to a cloud hosting environment, the Government expects to be using ECC v6.0 (Enhancement Pack 5, Service Pack 6), SAP Business Warehouse v7.3 SP5, XI/PI v7.3, NetWeaver Portal v7.3 (Enhancement Pack 1, Service Pack 7), and SAP Business Intelligence v4.0 (Service Pack 2), all on Solaris 10 and Oracle 11g. A portion of this ERP system, including PRISM v7.1, runs in a 64-bit Windows environment. The Government's preference is to continue running the SAP Application on a UNIX OS and Oracle RDBMS to mitigate the impact to custom programs and interface scripts. However, the Government is willing to consider different proposed operating system and hardware mixes as long as they (1) are SAP certified solutions according to the SAP Application PAMs, (2) can meet or exceed the SAPs, high availability, redundancy; scalability and performance requirements of the Program, and (3) can demonstrably run the FBMS infrastructure efficiently and cost effectively. The capabilities and risks associated with alternative operating system and hardware mixes should also be identified in the proposal and will be taken into consideration as part of the proposal evaluation. This is not meant to preclude consideration of an in-memory storage/processing solution, especially for the EMIS.

3.2. The FBMS infrastructure follows the standard N+1 SAP Landscape methodology utilizing the SAP 2-tier architecture in the Development landscapes and SAP 3-tier architecture in all other landscapes. FBMS is supported by the standard 5-box landscape for operations support and deployment (production, two development, and two test environments). In addition FBMS has training, production copy (PRODCOPY), and disaster recovery (DR) environments. FBMS is currently running in virtualized, clustered, and highly available configuration on Solaris with Sun Clustering.

3.3. The figures to follow are the projected requirements of FBMS over the next few years. These estimates were produced using the most current methods and models brought to bear by SAP, Oracle, the DOI's NBC, and the FBMS PMO (System Architect), and were validated by objective third-party review in January 2012.

3.4. PROCESSING CAPABILITY

3.4.1. Processing capability is represented in SAPS. The SAP Application Performance Standard (SAPS) is a hardware-independent unit of measurement that describes the performance of a system configuration in the SAP environment. It is derived from the Sales and Distribution (SD) benchmark, where 100 SAPS is defined as 2,000 fully business processed order line items per hour. In technical terms, this throughput is achieved by processing 6,000 dialog steps (screen changes), 2,000 postings per hour in the SD Benchmark, or 2,400 SAP transactions.

	FY13 (Memory currently installed)		FY14-FY15		FY16-FY17		FY18-FY19		FY20-FY21	
Environment	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)
Production	618,461	4,200	950,205	6,453	1,214,751	8,249	1,422,939	9,899	1,636,380	11,384
Training	20,904	830	22,995	913	25,294	1,005	27,887	1,105	32,070	1,271
Sandbox	104,447	794	125,337	952	137,870	1,048	152,002	1,152	174,802	1,325
DR	394,192	2,592	473,031	3,110	520,334	3,421	573,668	3,764	659,718	4,329
QAS1	394,192	2,592	473,031	3,110	520,334	3,421	573,668	3,764	659,718	4,329
QAS2	394,192	2,592	473,031	3,110	520,334	3,421	573,668	3,764	659,718	4,329
DEV1	108,491	672	130,189	806	143,208	887	157,887	976	181,570	1,122
DEV2	108,491	672	130,189	806	143,208	887	157,887	976	181,570	1,122
Totals	**2,143,370**	**14,944**	**2,778,008**	**19,260**	**3,225,334**	**22,339**	**3,639,606**	**25,400**	**4,185,547**	**29,210**

Table 1: SAPs required by Landscape supporting FBMS

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

Table 2 below provides the expected SAPs for each FBMS Production landscape application instance over the next several years.

System SAPs	Extrapolations through 5-Year Hardware Lifecycle		
	CY14-15	CY16-17	CY18-19
ECC	171,958	223,545	268,254
BW	265,645	345,338	414,406
BobJ	183,312	219,974	263,969
Portal	54,592	70,969	85,163
PI (XI)	7,090	9,217	9,217
GRC	7,850	9,027	9,930
Trex	683	887	887
PRISM	8,282	10,766	12,919
Web Proxy	331	431	517
SolMan	3,793	3,793	3,793
Opentext (aka IXOS)	7,591	10,000	12,000
SAP BusinesObjects Planning and Consolidation (BPC) 10.0 version for SAP Netweaver	53,129	69,068	75,974
SAP Public Budget Formulation (SAP PBF v8 or better = BW instance+Java Portal)	132,822	172,669	189,936
SAP BusinessObjects Profitability and Cost Management (SAP BOBJ PCM v7.5 or better)	53,129	69,068	75,974

Table 2: SAPs per Application in the FBMS Production Landscape through FY2019

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

FY2014-2015	Average SAPs estimates by tier			
PROD	**Apps**	**CS**	**DB**	**Total**
R/3	119,370	1,000	51,587	**171,957**
BW	184,951	1,000	79,693	**265,644**
Portal	42,673	1,000	10,918	**54,591**
XI	3,963	1,000	2,127	**7,090**
GRC	4,495	1,000	2,355	**7,850**
SolMan	2,035	1,000	759	**3,794**
PRISM	5,797	0	2,484	**8,281**
Opentext	6,073	0	1,518	**7,591**
SAP BobJ	127,318	1,000	54,994	**183,312**
SAP BobJ BPC	36,190	1,000	15,939	**53,129**
SAP PBF v8 or better	91,976	1,000	39,847	**132,823**
SAP BOBJ PCM v7.5 or better	36,190	1,000	15,939	**53,129**
Apache Webproxy	331			**331**
Trex	683			**683**
FY14-15 Average	**662,045**	**10,000**	**278,160**	**950,205**
Dep8 peak (20% spike)	**794,455**	**10,000**	**333,792**	**1,138,247**

Table 3: SAPs estimates per production instance by tier for FY2014-2015

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

3.5. STORAGE

Expected Total Usable Space @ year end (GB)	D8-FY14 (11/1/13-10/31/14)	FY15 (11/1/14-10/31/15)	FY16 (11/1/15-10/31/16)	FY17 10/31/17	FY18 10/31/18	FY19 10/31/19
Production	95,312	173,931	220,437	268,997	319,026	371,669
Backups PROD-BCV only	68,976	132,056	169,442	207,967	247,695	288,695
PROD Copy	95,312	173,931	220,437	268,997	319,026	371,669
Training	16,958	17,593	17,580	17,580	17,580	17,580
qas1	26,287	38,316	42,490	47,500	52,848	58,569
qas2	31,000	44,820	54,156	60,604	68,937	77,601
dev1	23,126	33,942	38,223	42,414	47,443	52,815
dev2	29,387	38,989	41,435	45,644	50,694	56,087
Disaster Recovery	95,312	173,931	220,437	268,997	319,026	371,669
Backups ESC-BCVs only	80,015	117,063	127,174	139,648	153,352	168,408

Table 4: Usable Storage by Landscape per year (cumulative)

Table 5. Projected Database Requirements through FY2015 by Environment

Projected Storage Requirements (GB)	ACTUAL		PROJECTED							
	D4 FY09-10 (11/1/08-10/31/10)	D5 FY11 (11/1/10-10/31/11)	D6 FY12 (11/1/11-10/31/12)	D7 FY13 (11/1/12-10/31/13)	D8 FY14 (11/1/13-10/31/14)	FY15 (11/1/14-10/31/15)	FY16 (11/1/15-10/31/16)	FY17 10/31/17	FY18 10/31/18	FY19 10/31/19
Production	6,131	11,060	25,192	63,195	95,312	173,931	220,437	268,997	319,026	371,669
Backups DDC-BCV only	3,513	6,926	13,568	43,791	68,976	132,056	169,442	207,967	247,695	288,695
Sandbox/PROD Copy	6,131	11,060	25,192	63,195	95,312	173,931	220,437	268,997	319,026	371,669
Training	15,758	15,758	15,758	16,958	16,958	17,593	17,580	17,580	17,580	17,580
qas1	10,901	16,752	19,774	21,370	26,287	38,316	42,490	47,500	52,848	58,569
qas2	13,262	19,114	21,503	25,574	31,000	44,820	54,156	60,604	68,937	77,601
dev1	11,309	16,952	17,726	20,145	23,126	33,942	38,223	42,414	47,443	52,815
dev2	13,703	19,874	19,952	26,293	29,387	38,989	41,435	45,644	50,694	56,087
Disaster Recovery	6,131	11,060	25,192	63,195	95,312	173,931	220,437	268,997	319,026	371,669
Backups ESC-BCVs only	19,776	58,536	62,347	71,272	80,015	117,063	127,174	139,648	153,352	168,408
Total	**106,615**	**187,092**	**246,204**	**414,988**	**561,685**	**944,572**	**1,151,811**	**1,368,348**	**1,595,627**	**1,834,762**

3.6. CPU AND MEMORY

3.6.1. Table 6 shows the projected CPU and memory requirements for all environments. The proposed solution should utilize the data in Table 6 for sizing.

		FY13 (currently own)		FY14		FY15		FY16		FY17		FY18	
	Environment	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)	Total SAPs	Total Memory (GB)
Denver	Production	618,461	4,200	950,205	6,453	950,205	6,453	1,214,751	8,249	1,214,751	8,249	1,422,939	9,899
	Training	20,904	830	22,995	913	22,995	913	25,294	1,005	25,294	1,005	27,887	1,105
	Sandbox	104,447	794	125,337	952	125,337	952	137,871	1,048	137,871	1,048	152,002	1,152
Herndon	DR & QAS1/QAS2	394,192	2,592	473,031	3,110	473,031	3,110	520,334	3,421	520,334	3,421	573,668	3,764
	DEV1/DEV2	108,491	672	130,189	806	130,189	806	143,208	887	143,208	887	157,887	976
	Totals	**1,246,495**	**9,088**	**1,701,757**	**12,234**	**1,701,757**	**12,234**	**2,041,458**	**14,610**	**2,041,458**	**14,610**	**2,334,383**	**16,896**

Table 6. Projected Total CPU and Memory Requirements through FY2015 by Landscape

3.7. RESPONSIBILITIES:

3.7.1. The current delineation of responsibilities in practice is shown in the table below. The hosting provider delivers data center infrastructure, network, server, and storage management along with infrastructure services, such as monitoring and alerting. The FBMS program manages and supports the business applications and related databases. It is anticipated that the hosting solution will reflect an equivalent split of responsibilities, unless a case is made for a different alignment. DOI shall retain the ability to monitor the cloud based containers/guests with its existing BMC installation.

Current Delineation of Responsibilities	
FBMS PMO	Hosting Provider
• Business application management • SAP technical application (BASIS) management • Lightweight Directory Access Protocol (LDAP) services • Domain Name System (DNS) management • Departmental network services • Security compliance and Information Assurance (IA) • Database administration • Production management and job control (Control-M)	• Core infrastructure services (DHCP, NTP, monitoring) • Server management and hardware administration (physical and virtual) • Storage management (NAS and SAN) • Non-DOI network services (routers, switches, firewalls, load balancing) • Facilities (power, cooling, floorspace, etc.) • OS management and patching • DBMS environment management and patching • Physical access controls

3.8. USER ACCESS

3.8.1. Table 7 shows the expected number of named users that have been or will be supported after each FBMS deployment.

FBMS Deployment	Named Users
D5	5,351
D6	9,511
D7	20,285
D8	21,872
FY2014	22,419
FY2015	23,540

Table 7. Planned Named User Counts per Deployment

3.8.2. FBMS serves an array of end-users nation-wide through the DOI's Enterprise Services Network (ESN). Given a change in hosting providers, the only change to connectivity will be the addition of one or more links from the new hosting provider into the DOI ESN and deletion of connections to the current provider.

3.9. DEPLOYMENT 8 AND BEYOND

3.9.1. New SAP instances are planned as part of D8 and as a FY2014 release. SAP Business Planning and Consolidation (BPC) or an equivalent application is targeted for D8 with a sizing estimate of 20% of the existing SAP BW resources. This is based on the ratio of users that will be on this new BW system compared to those on the existing BW. Instances for SAP Public Budget Formulation (PBF) and SAP Profitability and Cost Management (PCM), or equivalent applications, are being considered for FY2014 deployment, subject to approval of governance groups, and were sized as a percentage of existing system types based upon expected user ratios.

- SAP BPC equivalent to 20% of SAP BW requirements
- SAP PBF equivalent to 50% of SAP BW requirements
- SAP PCM equivalent to 20% of SAP BW requirements

3.9.2. D8 completes the planned initial roll outs to DOI bureaus. Afterwards, performance will be impacted by release upgrades and data growth. SAP typically publishes a note with a new release recommending between a 5% and 10% increase in system resources in order to maintain performance. With the accumulation of data records, there will also be a decrease in performance. These two factors are accounted for with a total estimated percentage increase in SAPs and memory requirements between 10% and 30% for FY2014/2015. This

estimate may be refined as additional information on the targeted release and SAP recommendations on additional capacity requirements for said release become clearer.

4. PERFORMANCE REQUIREMENTS

4.1. FBMS HOSTING: The contractor shall provide infrastructure services in order to host all components and instances of FBMS as constituted at the conclusion of D8, provisioning the necessary processing (Table 6), memory (Table 6), storage (Table 5), and bandwidth so as to maintain or improve upon current service levels throughout the period of performance as stated herein.

4.2. HOSTING ASSETS: The infrastructure services shall be provisioned using hosting assets that are fully virtualized, clustered, and in a highly-available, fault-tolerant configuration, as the terms are generally understood in the industry. The contractor shall be able to incorporate new industry technologies (such as in-memory appliances, Web/Network accelerators, and security devices) into the environment as they become commercially available, to maintain acceptable service levels, response times, and costs given the expected system growth.

4.3. CLOUD COMPUTING: The contractor shall comply with the NIST definition of cloud computing as outlined in NIST Special Publication 800-145, specifically:

4.3.1. On Demand Self-Service. The government can unilaterally provision computing capabilities, such as server time and storage, as needed, without requiring human interaction with the service provider.

4.3.2. Broadband Network Access. As user access to FBMS will be delivered and managed through DOI internal networks, this aspect of the NIST definition does not apply.

4.3.3. Resource Pooling. The service provider's computing resources are pooled to serve multiple customers using a multi-tenant model, with different resources dynamically assigned and reassigned according to demand. That said, FBMS requires geographical separation of the production (PROD) and disaster recovery (DR) landscapes, as is now the case.

4.3.4. Rapid Elasticity. Capabilities can be rapidly and elastically provisioned to quickly scale up, both horizontally and vertically, and rapidly released to quickly scale down. The capabilities available appear to be unlimited and can be purchased in any quantity at any time.

4.3.5. Measured Service. Capacity and activity are measured and reported automatically. Charges are based upon metered services that are monitored, controlled, and reported, providing transparency for both the provider and the government.

4.4. SOFTWARE: Software used to provide the infrastructure services shall be kept current with the most recent patches, versions, service packs, upgrades, etc.

4.5. HARDWARE: Hardware used shall be sufficiently current and capable so as to maintain the Acceptable Quality Levels detailed below. Appliances and/or engineered point solutions used to increase response times shall be employed as they become commercially available.

4.6. STORAGE: Storage used to provision the infrastructure services shall be tiered and sufficiently current and capable so as to maintain the Acceptable Quality Levels detailed below.

4.7. AUTOMATED STATUS REPORTING: Automated reporting mechanisms shall be provided to provide transparency into each of the Acceptable Quality Level metrics enumerated below, and into every metered service upon which billing is based or which may affect performance. To facilitate diagnostics and troubleshooting, all monitoring and reporting activities currently performed for FBMS by the NBC, including daily "Health Check" processing, (see attachment A) shall be replicated or replaced by equivalent metrics. The government shall have continuous and unrestricted access to such reporting mechanisms, without need for intervention by the service provider.

4.8. SAP CERTIFICATION: The service provider shall be a certified SAP Certified Cloud Services Provider.

4.9. CONTINGENCY RESPONSE: The infrastructure service shall provide such back-up/restoration, disaster recovery, and continuity of operations processes as will guarantee the disaster response acceptable quality level, described below.

4.10. INCENTIVES/DISINCENTIVES: The service provider shall structure and manage its underlying assets so as to guarantee satisfaction of the Acceptable Quality Levels described below. Failure to meet one or more of the acceptable quality levels in any month shall cause the service provider to incur forfeiture of a percentage of the scheduled billed amount in the next billing cycle.

5. ACCEPTABLE QUALITY LEVELS:

5.1. AVAILABILITY. The percentage of time that the provided infrastructure services supporting FBMS shall be functioning and available to the end users on a 24-hours-per-day/seven-days-per week basis, excluding agreed-upon maintenance periods, shall not fall below 99.9% (measured over one month). Availability shall not fall below 99.999% during the months of August, September, and October of each year. Availability will be evaluated on a monthly basis for determining compliance with the task order.

5.2. RELIABILITY. Mean Time to Recovery (MTTR) – the period from the time an error condition is discovered until it is resolved - for all system outages attributable to infrastructure failure shall not exceed 60 minutes. Error conditions shall be reported promptly upon discovery. MTTR will be evaluated on a monthly basis for determining compliance with the task order.

5.3. USAGE AND RESPONSE TIME. Daily average CPU usage (overall and for any FBMS application) shall not exceed 70%. Daily average memory utilization (overall and for any platform used by FBMS) shall not exceed 70%. Daily average network utilization shall not exceed 30%. Daily average database execution time shall not exceed two seconds. Usage and response times will be evaluated monthly for determining compliance with the task order.

5.4. DISASTER RESPONSE. Backup and recovery services shall support a Recovery Time Objective (RTO) not to exceed 48-hours, and a Recovery Point Objective (RPO) not to exceed 6-hours. RTO and RPO will be evaluated after each back-up and recovery evolution, and during scheduled disaster recovery testing.

5.5. RESOURCE PROVISIONING. The provisioning and release of resources (scaling up and down of CPU, memory, storage, or network bandwidth) shall not exceed 72 hours. Provisioning and release times will be evaluated after each scaling evolution.

6. CONSTRAINTS

6.1. TERMS OF SERVICE. Any terms of service must comply with federal law and agency regulation. Conflicts will be resolved in favor of the government's requirements and/or terms and conditions.

6.2. NON-DISCLOSURE. Service provider employees performing activities are required to sign appropriate non-disclosure agreements. Service provider employees may be exposed to data pertaining to other contracts and services in the course of their duties. The service provider shall not divulge this information or use this information for gain and shall not divulge any information to any person without written permission from the Contracting Officer and FBMS COTR.

6.3. SECURITY. The hosting environment provisioned by the service provider must demonstrate an appropriate level of security by meeting the requirements of Section C.5.3.1 of the IDIQ Contract. The continuous monitoring provided must comply with the NIST Special Publication 800-137 framework and Department of Homeland Security (DHS) guidance.

6.4. INCIDENT RESPONSE. The service provider shall have, and exercise annually, an incident response plan to address security or privacy breaches, data loss, and unauthorized access to data. Such plan will comply with FISMA, the Trusted Internet Connection (TIC) initiative, ISO 27001, NIST standards, and related agency policies.

The service provider shall adhere to U.S. Computer Emergency Readiness Team (US-CERT) guidance on incidence response and threat notifications.

6.5. PRIVACY. The services provided shall comply with the provisions of the Privacy Act of 1974, especially with regard to the handling and protection of Personally Identifiable Information (PII). The service provider shall cooperate in the conduct of periodic Privacy Impact Assessments (PIA), as required by Section 208 of the e-Government Act of 2002.

6.6. DATA LOCATION. The service provider shall not host any portion of the FBMS environment in facilities outside the contiguous United States, Alaska, Hawaii, and other U.S. Territories.

6.7. DATA OWNERSHIP. All data used by or contained in FBMS is the property of the government of the United States, as specified in FAR 52.227.14, Rights in Data-General (DEC 2007).

6.8. OPERATING ENVIRONMENT. The current environment is running in UNIX OS and Oracle RDBMS. However, the Government is willing to consider different proposed operating system and hardware mixes as long as they (1) are SAP certified solutions according to the SAP Application PAMs, (2) can meet or exceed the SAPs, high availability, redundancy; scalability and performance requirements of the Program, and (3) can demonstrably run the FBMS infrastructure efficiently and cost effectively. The capabilities and risks associated with alternative operating system and hardware mixes should also be identified in the proposal and will be taken into consideration as part of the proposal evaluation. This is not meant to preclude consideration of an in-memory storage/processing solution, especially for the EMIS.

7. PROJECT MANAGEMENT AND REPORTING

7.1. The Project Manager (PM) shall meet monthly, or as requested, with the FBMS Contracting Officer's Technical Representative (COTR) to review action items, discuss progress to date, and review upcoming planned activities. Any changes needed to the work plan will be discussed and agreed to. Commencement of changes shall not occur until a modification to the Task Order has been executed by the Contracting Officer.

7.2. The service provider shall provide weekly status reports to ensure that its expenditure of resources is consistent with and will lead to successful completion of all tasks within projected cost and schedule limitations. Such status reports shall detail progress made since the last report, progress expected during the current reporting period, proposed resources, significant problems or issues encountered, and recommended actions to resolve them.

8. PERSONNEL REQUIREMENTS

8.1. Each employee of the service provider working on the task order shall either be a citizen of the United States of America or hold lawful permanent resident status.

8.2. The staff assigned to this program shall collectively have the following qualifications:

- Expert knowledge of and substantial experience with SAP installations
- Knowledge of and experience in working with federal government agencies
- Knowledge of current industry trends and developments regarding ERP implementations, Enterprise Architecture, cloud computing and storage, to include emerging technologies such as web/network accelerators and in-memory appliances.

8.3. The Service provider personnel assigned to this program must comply with all DOI security rules and must provide evidence of appropriate clearances (for example, HSPD-12) for access to and processing of sensitive, proprietary, and mission critical data. Names and identification information must be provided to the FBMS COTR for each person working on this project so that DOI security can perform the required National Agency Check with Inquiries (NACI) prior to the commencement of work.

8.4. All documents prepared by the service provider shall be on behalf of the FBMS Program and the service provider shall not publish or distribute any document without prior written permission from the Contracting Officer and the FBMS COTR. The service provider shall review and provide written comments on the technical accuracy and completeness of all final deliverables. No documents, reports, information, etc. may be released to the public or provided to any party without prior written approval of the Contracting Officer and the FBMS COTR.

9. TRAVEL

Travel by the contractor in support of this task order will be reimbursed by DOI provided:

(a) The specific travel is authorized in writing by the DOI COTR. The format and process for receiving travel authorizations will be communicated at the award kickoff meeting. The contractor shall provide the COTR adequate time to review and approve travel plans. Note that no travel expenses will be reimbursed without prior written approval by the COTR.

(b) All travel costs and per diem costs must conform to Federal Travel Regulations (FTR) in effect at the time of travel authorization, including to but not limited to daily per diem and lodging rates in effect for the area at the time of the travel. Expenses not in conformity with the FTR will not be reimbursed and should not be submitted.

(c) Receipts and other written evidence to support submitted travel expenses over $25.00 will be retained by the contractor for the duration of the award plus one year, and made available to the CO or COTR on request. Travel not supported by receipts or other evidence will not be

reimbursed and should not be submitted. The contractor will state on all invoices that include claims for travel reimbursement that these claims are fully supported by proper documentation, that the documentation is available for audit, and that the claims conform to the FTR.

10. DELIVERY SCHEDULE

10.1. Work to be accomplished during the first year is anticipated to be at least the following: (1) Conduct of a comprehensive cloud readiness assessment of the FBMS technical infrastructure and program, (2) collaborative crafting of a detailed cloud hosting transition plan, (3) execution of a pilot transition of a complete FBMS environment to the cloud hosting infrastructure service for testing and eventual production, and (4) execution of additional parts of the detailed transition plan, as schedule may allow.

10.2. When the base period project plan is approved, by the Government, the agreed-upon deliverables and milestones displayed below will be updated with the approved target dates. When so populated, the table below will delineate the delivery schedule for contractor support. The base period project plan will contain a detailed description of the development of the deliverables.

10.3. The service provider shall deliver all products concurrently to the FBMS COTR and the Contracting Officer. Electronic transmission will be the primary delivery mechanism, however hard copies will also be provided, as requested. The FBMS COTR will notify the Contractor of deliverable acceptance or provide comments in writing within five (5) government workdays of receipt of a deliverable. Within five (5) government workdays, the Contractor shall resubmit the final deliverable to the FBMS COTR and Contracting Officer, if necessary.

10.4. The base period project plan shall be submitted to the FBMS COTR before other work (other than the cloud-readiness evaluation) commences, and no later than 30 days after the award of this contract, unless otherwise directed by the COTR. The base period project plan will be evaluated by the COTR for quality of content, timeliness, and clarity.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

Deliverable or Milestone	Schedule
Production of the base period project plan with milestones	Draft submission within 30 calendar days of award
Cloud-readiness evaluation of the FBMS infrastructure and program	As established in the approved base period project plan, but within 60 calendar days of award
Finalize the proposed Quality Assurance Plan with the PMO and secure approval	As established in the approved base period project plan, but within 60 calendar days of award
Preparation of the cloud hosting transition plan in collaboration with the FBMS Program Management Office	As established in the approved project plan, but within 90 calendar days of award
Pilot transition of an FBMS environment to the cloud hosting service and pilot testing	As established in the approved project plan.
Management of the FBMS cloud transition and testing	As established in the cloud hosting transition plan
Ongoing Infrastructure-as-a-Service operations management	As established in the cloud hosting transition plan
Monthly Progress Meeting (Section 8.1)	Monthly, as mutually agreed upon
Weekly Status Reports (Section 8.2)	Close-of-business each Friday

11. GOVERNMENT FURNISHED EQUIPMENT AND MATERIALS

Government-furnished property (materials, equipment, software applications, software licenses/software maintenance agreements and/or information) may be provided in conjunction with required performance under this task order as determined by mutual agreement between the Government and the Contractor. At the written request of the Government, the Contractor shall immediately return any property provided by the Government for the Contractor's use in completing the assigned tasks. If not requested, the Contractor shall continue to abide by FAR part 45 until completion of the task order.

12. PLACE OF PERFORMANCE

The service provider shall host FBMS using its own resources. The serviced provider may be required to travel occasionally to the FBMS Project Management Offices in Herndon, Virginia and Lakewood, Colorado, or at DOI's Main Interior Building in Washington D.C., when required by the Government.

13. PERIOD OF PERFORMANCE

The period of performance shall be from the date of task order award for eight years (a two-year base period and two three-year option periods). Exercising of any of the option periods is contingent upon the contractor having a current IDIQ contract at the time the option is exercised. All terms and conditions applicable to the base period shall extend to the options unless

otherwise agreed upon. The option periods are subject to the availability of funds. The Government shall not be obligated to reimburse the Contractor for costs in excess of the amount allotted, nor will the Contractor be obligated to continue performance and incur costs in excess of the amount allotted.

14. OTHER DIRECT COSTS

Other direct costs require government pre-approval by means of a properly executed contract document or modification.

15. CONTRACT ADMINISTRATION

15.1. All payment requests must be submitted by Suppliers electronically through the U.S. Department of the Treasury's Invoice Processing Platform System (IPP). The U.S. Department of the Treasury Financial Management Service (FMS), in partnership with the Federal Reserve Bank of Boston (FRBB), a fiscal agent of the U.S. Treasury, is offering the IPP service for use by Federal Government and their suppliers at no charge. The IPP facilities the conversion of paper-based processes to electronic interactions by providing a Web-based portal for easy data access at no charge to Agencies and their suppliers. NOTE: The IPP is the Department of Interior (DOI) preferred method of submitting invoices for payment. "Payment request" means any request for contract financing payment of invoice payment by the Supplier. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Payment documentation and Process" and FAR 52.232-25.

15.2. Suppliers can enroll to access and use IPP for submitting requests for payment by going to the website at https://www.ipp.gov/. Supplier assistance with enrollment can be obtained by contacting the FBMS Customer Support Desk at 703-793-5575 or email FBMS_IPP@FBMS.doi.gov.

15.3. If your firm is unable to comply with using IPP for submitting invoices for payment due to lack of an account with a financial institution; a physical or mental disability; a geographic, language, or literacy barrier; or a financial hardship, then you must inform the contracting officer orally or in writing. Your invoice needs to be attached to the IPP submittal in order to be processed for payment.

16. TECHNICAL CONTACTS

Contracting Officer's Technical Representative:

** TBD at Kickoff Meeting*

17. ORGANIZATIONAL CONFLICT OF INTEREST

Contractor employees shall be required to sign a standard FBMS non-disclosure agreement as a condition of employment on the project. Contractor employees may also be required to sign a Conflict of Interest certificate if the Contracting Officer determines that the task order and associated work may potentially affect the employee's financial interest.

18. FAR 217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to the expiration of the current period of performance.

(End of clause)

19. FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a) The Government may extend the term of this contract by written notice to the Contractor within 30 DAYS provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 DAYS before the contract expires. The preliminary notice does not commit the Government to an extension.
b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed eight (8) years.

(End of clause)

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 | 2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
0001	09/27/2013		

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
Interior Business Center, AQD Division 2 /Branch 3 381 Elden St Suite 4000 Herndon VA 20170	D23	DOI, Interior Business Center, AQD Division 2/Branch 3 381 Elden St Suite 4000 Herndon VA 20170	D23

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

UNISYS CORPORATION
Attn: ATTN GOVERNMENT POC
11720 PLAZA AMERICA DR TOWER III
RESTON VA 20190-4757

CODE 0070334821 FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

x 10A. MODIFICATION OF CONTRACT/ORDER NO.
D13PC00025
D13PD00827

10B. DATED (SEE ITEM 13)
05/01/2013

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) Net Increase: $2,365,444.00

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) Incremental Funding - Mutual Agreement of the Parties

E. IMPORTANT: Contractor ☐ is not ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to:

1. Incrementally fund the base period of performance in the amount of $2,365,444.00 through 04/30/2015.

2. Change the date as stated in block 17(b) of the award document from April 2, 2013 to April 8, 2013, as the date was incorporated incorrectly at the time of award.

3. Identify and incorporate the contractor's Project Manager, Ronald Wenner, for the task order identified in block 10A above.

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Melanie Crouch, Sr. Contracts Mgr.	Terrie Callahan

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
Melanie Crouch (Signature of person authorized to sign)	9/27/2013	(Signature of Contracting Officer)	09/27/2013

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

NAME OF OFFEROR OR CONTRACTOR
UNISYS CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	4. Incorporates by reference the following Government accepted deliverable plans as identified in Section 10 of the task order: Quality Assurance Plan, dated 6/14/13, Cloud Readiness Assessment Document, dated 8/8/13, and Cloud Hosting Transition Plan, dated 8/26/13. As a result of this modification, the total obligated amount to the Base period of performance is hereby increased from $2,298,990.00 by $2,365,444.00 to $4,664,434.00. Additional funding may be provided during the Base period of performance in the amount of $4,994,647.91 to fully fund the Base period. However, the Government shall not be obligated to reimburse the contractor for expenses incurred in the excess of the current allotment, nor will the contractor be obligated to continue performance and incur cost in excess of the amount provided. The overall value of the Base period of performance remains unchanged in the amount of $9,659,081.91. The overall value of this task order remains unchanged in the amount of $43,948,773.00 (Base and all options, if exercised). ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED. Payment Terms: ACCP FOB: Destination Period of Performance: 05/01/2013 to 04/30/2015 Add Item 00020 as follows:				
00020	SAP Application Hosting - Incremental Funding				2,365,444.00
	All terms and conditions applicable to the IDIQ Contract No. D13PC00025 are applicable to this task order and any/all subsequent modifications unless otherwise agreed upon.				

SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE	OF PAGES
		1	73

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NO.
D13PC00025	D12PS00316	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	07/18/2012	0040073246

7. ISSUED BY	CODE	8. ADDRESS OFFER TO *(If other than Item 7)*
Department of the Interior, Acquisition Services Directorate Attn: Terrie L. Callahan, 703-964-3596, Terrie_Callahan@nbc.gov 381 Elden Street, Suite 4000 Herndon, Virginia 20170-4817		**Terrie L. Callahan, Contracting Officer** **(See Block # 7 for additional information)**

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder"

SOLICITATION

9. Sealed offers in original and copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if handcarried, in the depository located in _____ until _____ local time _____.

CAUTION — LATE Submissions, Modifications, and Withdrawals: See Section L. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)* AREA CODE	NUMBER	EXT.	C. E-MAIL ADDRESS
	TERRIE L. CALLAHAN	703	964-3596		Terrie_Callahan@nbc.gov

11. TABLE OF CONTENTS

(✓)	SEC.	DESCRIPTION	PAGE(S)	(✓)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	9
X	B	SUPPLIES OR SERVICES AND PRICE/COST	2			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS /WORK STATEMENT	46	X	J	LIST OF ATTACHMENTS	525
X	D	PACKAGING AND MARKING	1			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
X	E	INSPECTION AND ACCEPTANCE	2		K	REPRESENTATIONS, CERTIFICATIONS	
X	F	DELIVERIES OR PERFORMANCE	4			AND OTHER STATEMENTS OF OFFERORS	
X	G	CONTRACT ADMINISTRATION DATA	10		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	10		M	EVALUATION FACTORS FOR AWARD	

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 90 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232-8)*	10 CALENDAR DAYS %	20 CALENDAR DAYS %	30 CALENDAR DAYS %	CALENDAR DAYS %

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*
Unisys Corporation 11720 Plaza America Dr., Reston, VA 20109			Joy J. Scrimshire Director, Contracts

15B. TELEPHONE NUMBER AREA CODE	NUMBER	EXT.	☐ 15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE
				Joy J. Scrimshire	5/1/2013

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION
	$5,000	

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: ☐ 10 U.S.C. 2304(c) ( ) ☐ 41 U.S.C. 253(c)( )	23. SUBMIT INVOICES TO ADDRESS SHOWN IN	ITEM
	SEE SECTION G.2.2	

24. ADMINISTERED BY *(If other than Item 7)*	CODE	25. PAYMENT WILL BE MADE BY	CODE

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA *(Signature of Contracting Officer)*	28. AWARD DATE
TERRIE L. CALLAHAN	Terrie L Callahan	5/1/2013

IMPORTANT -- Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE 1	OF PAGES 73

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NO.
D13PC00025	D12PS00316	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	07/18/2012	0040073246

7. ISSUED BY	CODE	8. ADDRESS OFFER TO *(If other than Item 7)*
Department of the Interior, Acquisition Services Directorate Attn: Terrie L. Callahan, 703-964-3596, Terrie_Callahan@nbc.gov 381 Elden Street, Suite 4000 Herndon, Virginia 20170-4817		Terrie L. Callahan, Contracting Officer (See Block # 7 for additional information)

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder"

SOLICITATION

9. Sealed offers in original and copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if handcarried, in the depository located in _____ until _____ local time _____.

CAUTION — LATE Submissions, Modifications, and Withdrawals: See Section L. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)* AREA CODE	NUMBER	EXT.	C. E-MAIL ADDRESS
	TERRIE L. CALLAHAN	703	964-3596		Terrie_Callahan@nbc.gov

11. TABLE OF CONTENTS

(✓)	SEC.	DESCRIPTION	PAGE(S)	(✓)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	9
X	B	SUPPLIES OR SERVICES AND PRICE/COST	2			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	46	X	J	LIST OF ATTACHMENTS	525
X	D	PACKAGING AND MARKING	1			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
X	E	INSPECTION AND ACCEPTANCE	2		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
X	F	DELIVERIES OR PERFORMANCE	4				
X	G	CONTRACT ADMINISTRATION DATA	10		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	10		M	EVALUATION FACTORS FOR AWARD	

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 90 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232-8)*	10 CALENDAR DAYS %	20 CALENDAR DAYS %	30 CALENDAR DAYS %	CALENDAR DAYS %

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*
Unisys Corporation 11720 Plaza America Dr., Reston, VA 20109			Joy J. Scrimshire Director, Contracts

15B. TELEPHONE NUMBER AREA CODE	NUMBER	EXT.	☐ 15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE
					5/1/2013

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION
	$5,000	

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: ☐ 10 U.S.C. 2304(c) ( ) ☐ 41 U.S.C. 253(c)( )	23. SUBMIT INVOICES TO ADDRESS SHOWN IN SEE SECTION G.2.2	ITEM

24. ADMINISTERED BY *(If other than Item 7)* CODE	25. PAYMENT WILL BE MADE BY CODE

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA *(Signature of Contracting Officer)*	28. AWARD DATE
TERRIE L. CALLAHAN	Terrie L. Callahan	5/1/2013

IMPORTANT -- Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE 1	OF PAGES 73

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NO.
D13PC00025	D12PS00316	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	07/18/2012	0040073246

7. ISSUED BY	CODE	8. ADDRESS OFFER TO *(If other than Item 7)*
Department of the Interior. Acquisition Services Directorate Attn: Terrie L. Callahan, 703-964-3596, Terrie_Callahan@nbc.gov 381 Elden Street. Suite 4000 Herndon, Virginia 20170-4817		**Terrie L. Callahan, Contracting Officer** **(See Block # 7 for additional information)**

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder"

SOLICITATION

9. Sealed offers in original and copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if handcarried, in the depository located in _____ until _____ local time _____.

CAUTION — LATE Submissions, Modifications, and Withdrawals: See Section L. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)* AREA CODE	NUMBER	EXT.	C. E-MAIL ADDRESS
	TERRIE L. CALLAHAN	703	964-3596		Terrie_Callahan@nbc.gov

11. TABLE OF CONTENTS

(✓)	SEC.	DESCRIPTION	PAGE(S)	(✓)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	9
X	B	SUPPLIES OR SERVICES AND PRICE/COST	2			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	46	X	J	LIST OF ATTACHMENTS	525
X	D	PACKAGING AND MARKING	1			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
X	E	INSPECTION AND ACCEPTANCE	2		K	REPRESENTATIONS, CERTIFICATIONS	
X	F	DELIVERIES OR PERFORMANCE	4			AND OTHER STATEMENTS OF OFFERORS	
X	G	CONTRACT ADMINISTRATION DATA	10		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	10		M	EVALUATION FACTORS FOR AWARD	

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 90 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232-8)*	10 CALENDAR DAYS %	20 CALENDAR DAYS %	30 CALENDAR DAYS %	CALENDAR DAYS %

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*
Unisys Corporation 11720 Plaza America Dr., Reston, VA 20109			

15B. TELEPHONE NUMBER AREA CODE	NUMBER	EXT.	☐ 15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION
	$5,000	

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: ☐ 10 U.S.C. 2304(c) ( ) ☐ 41 U.S.C. 253(c)( )	23. SUBMIT INVOICES TO ADDRESS SHOWN IN	ITEM
	SEE SECTION G.2.2	

24. ADMINISTERED BY *(If other than Item 7)*	CODE	25. PAYMENT WILL BE MADE BY	CODE

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA	28. AWARD DATE
TERRIE L. CALLAHAN	Terrie L Callahan *(Signature of Contracting Officer)*	5/1/2013

IMPORTANT -- Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

This requirement is being issued by the Department of the Interior (DOI)/National Business Center (NBC), Acquisition Services Directorate (AQD) on behalf of the DOI, Office of the Chief Information Officer (CIO). This particular contract provides for cloud services, as specified in Section C, Description/Specifications/Work Statement, for the DOI. Also, this vehicle allows request for quotes/task orders to be issued on behalf of other government customers including both civilian agencies and the Department of Defense, by AQD Contracting Officers, in accordance with the Office of Management and Budget's (OMB) memorandum dated September 29, 2011. As future requirements are identified, it is critical the DOI has a ready contract vehicle in place for its use as well as customer agencies with an immediate need for these types of requirements.

This is an Indefinite-Delivery-Indefinite-Quantity (IDIQ), fixed price per "unit of service" type vehicle(s) within the various service areas.

Any specific tasks, above those already identified within the general categories currently specified in Section C, Description/Specifications/Work Statement and Section B, Supplies or Services and Prices/Costs are considered within scope of this contract, and will be performed under separate delivery/task orders and/or changes orders as appropriate. For example, if a task order requires support services for any portion and a labor category specific to the individual task order is not in the current IDIQ, it would allow the contractor to propose, and the Government to negotiate, the inclusion of the labor category. This could also pertain to an offering that is considered within the general scope but not explicitly identified within the pricing.

For task orders issued against this contract the order request will originate from AQD Contracting Officer and will identify the scope of work required and any additional instructions regarding proposal submission. All orders shall use the rates established herein.

The contractor shall furnish all personnel, facilities, equipment, materials, supplies, and/or services in performing the work described in Section C and Section J, Attachments, and any subsequent orders issued under this contract, unless otherwise stated herein. Orders will be issued for fixed-price units of service unless otherwise agreed upon in the individual task orders.

B.2 NORTH AMERICAN INDUSTRICAL CLASSISIFICATION CODE (NAICS)

The following North American Industry Classification Code (NAICS Codes) is the primary code applicable to this acquisition: 541519 (Other Computer Related Services), business size standard of $25 Million.

B.3 PRICING SCHEDULES

The Contractor shall utilize pricing for subsequent task orders as established within this contract as reflected in the base period and each of the option periods in accordance with Fixed Price (FP) Unit of Service (UoS). Pricing for this task order includes each of the Service Line(s) identified below.

- Storage Services
- Secure File Transfer Services
- Virtual Machine Services
- Database Hosting Services
- Web Hosting Services
- Development and Test Environment Services
- SAP Application Hosting Services

The FP UoS applicable to the technical services lines identified and any associated labor categories and loaded rates to be utilized on task orders placed against this contract are hereby in accordance with the Contractor's pricing proposal dated November 19, 2012, submitted in response to the Foundation Cloud Hosting Solicitation, D12PS00316, which is hereby incorporated by reference with the same force and effect as if included in full text.

Any inconsistencies or in the event of a conflict between and terms and conditions of this contract and the contractor's proposal shall be resolved by giving precedence to the terms and conditions contain in this contract.

B.4 OTHER DIRECT COSTS (ODCs)

Other Direct Costs, not identified herein, shall be task order dependent. The price(s) charged to the government for such item(s) or service(s) shall be procured in accordance with all required laws and regulations. The contractor shall seek competitive bids for all lots of equipment, supplies, and/or services exceeding the micro-purchase threshold, as identified in the Federal Acquisition Regulation (FAR) 2.1, Definitions, which are acquired under this contract, and provide them to the government as backup documentation to support price reasonability.

B.5 MINIMUM AND MAXIMUM THRESHOLDS

During the life of this contract, the government is not obligated to purchase services above the guaranteed minimum for this entire period of performance for this IDIQ (inclusive of options) which is $5,000.

The contract ceiling for this entire period of performance for this IDIQ (inclusive of options) is $1,000,000,000.

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 EXECUTIVE OVERVIEW

This contract defines the requirements for services supporting Foundation Cloud Hosting requirements, which align with the Department of the Interior's (DOI) IT Transformation efforts.

The DOI's IT Transformation efforts are designed to align with the "25-point Implementation Plan to Reform Federal IT", the Federal Datacenter Consolidation Initiative ("FDCCI"), and the Cloud-First Policy outlined by the Federal Chief Information Officer ("CIO"). Federal IT Transformation efforts are designed to address two primary objectives:

1. Reduce the total cost of ownership of datacenter hosting hardware, software and operations; and
2. Provide greater service, security and support for application business owners and end-users.

The DOI's goal is to establish the most, efficient, effective and transparent portfolio of IT service delivery solutions for meeting mission needs utilizing modern technology.

Initially, the DOI is seeking cloud-based services in the following seven (7) technical service lines:

- Storage Services
- Secure File Transfer Services
- Virtual Machine Services
- Database Hosting Services
- Web Hosting Services
- Development and Test Environment Hosting Services
- SAP Application Hosting Services

These technical service lines are intended to establish the initial infrastructure foundation for developing composite services that will be represented in a "Mission-Facing", DOI-Wide IT Services Catalog.

Additionally, the DOI considers Data Center Consolidation or emergency operations requirements, and any hosting and associated support services necessary, to be within scope of this contract. Therefore, any modifications and/or task orders maybe be executed for any requirements within this area. This would include Contractor operation and maintenance of Government owned assets within either Government or Contractor owned and operated facilities.

C.2 OBJECTIVES

C.2.1 Business Objectives

The DOI's business objectives for the IT Service Delivery program are as follows:

a. Improve availability, performance, and flexibility of datacenter services;
b. Reduce Total Cost of Ownership ("TCO") of delivering IT services;
c. Promote the use of Green IT by reducing the overall energy, real estate footprint, and use of toxic components of DOI datacenters, and implementing effective recycling and reuse programs;
d. Ensure all applicable federal information security and privacy regulations are maintained and adhered to;
e. Provide tiered functions, service levels, and performance for customers;
f. Provide interoperable and portable solutions that enable mobility across hosting models and service providers; and
g. Enable scaling of infrastructure and application resources to meet evolving application and user demand.

C.2.2 Initial Technical Service Lines

The DOI is seeking cloud-based services in the following seven (7) technical service lines. These technical service lines are intended to establish the initial infrastructure foundation for developing composite services that will be represented in a "Mission-Facing", DOI-Wide IT Services Catalog

C.2.2.1 Storage Services

The Storage Services Technical Service line includes, but is not limited to Cloud Based Storage Services in support of the DOI Continuity of Operations (CoOP), Disaster Recovery (DR), and Data Center Consolidation Transition Support Requirements.

C.2.2.2 Secure File Transfer Services

The Secure File Transfer Service Technical Service Line includes, but is not limited to an enterprise-wide capability for any employee, contractor or partner working on the DOI network to securely transfer files of any size and type to either internal or external business partners. This includes the capability for DOI employees, contractors and partners to receive files of any size and type from external business partners, while maintaining confidentiality and integrity, and the ability to manage the files in a web environment.

C.2.2.3 Virtual Machine Services

The Virtual Machine Services Technical Service Line includes, but is not limited to Cloud Based Virtual Machine Services in support of the Data Center Consolidation Transition Support and New Application Implementation Requirements. This Service Line may also be considered as an

alternative to technical refresh of physical servers, a quick response resource to explore innovation opportunities, or rapid response multiprocessor multi-machine simulation environment.

C.2.2.4 Database Hosting Services

The Database Hosting Services Technical Service Line includes, but is not limited to, Cloud Based Database Hosting Services in support of the DOI Data Center Consolidation Transition and New Application Implementation Requirements. This service line may include stand-alone databases, shared data sources, or tiered database solutions including components of one or more other Technical Service Lines.

C.2.2.5 Web Hosting Services

The Web Hosting Services Technical Service Line includes, but is not limited to cloud Based Web Hosting Services in public, private, community and hybrid cloud environments. This service line may include any combination of other Technical Service lines necessary to deliver static and/or dynamic information to the DOI stakeholders, and includes hosting for an enterprise-wide content management system.

C.2.2.6 Development and Test Environment Hosting Services

The Development and Test Environment Hosting Service includes, but is not limited to providing a flexible, scalable, on-demand environment to support development, testing, staging, and/or quality assurance before releasing new applications and changes into the DOI production environment. They also support ad-hoc innovation activities. Change Control and User Permissions in this non-production environment are typically established on an instance by instance basis by the authorized user who provisioned the service.

C.2.2.7 SAP Application Hosting Services

The purpose of SAP Application Hosting Services is to acquire cloud-based Infrastructure-as-a Service hosting and associated transition support for the Department of the Interior's Financial and Business Management System (FBMS), to include suitability/readiness assessment, conversion planning, implementation management, and infrastructure operations.

C.3 INTRODUCTION TO TECHNICAL SERVICE DEFINITION MODEL

All technical services must fulfill a set of common, enterprise-wide requirements. Within each service line, technical services are defined based upon three dimensions: 1) Resource Requirements, 2) Service Level Requirements, and 3) Optional Characteristics Requirements. Additionally, each service line may require Associated Support Services to enable efficient migration from the current operating environment to the target operating environment, or to support sustained operations and maintenance of systems in the target operating environment. ***Figure 1 DOI IT Service Delivery Requirements*** below illustrates how these requirements and service dimensions fit together to define a Technical service.

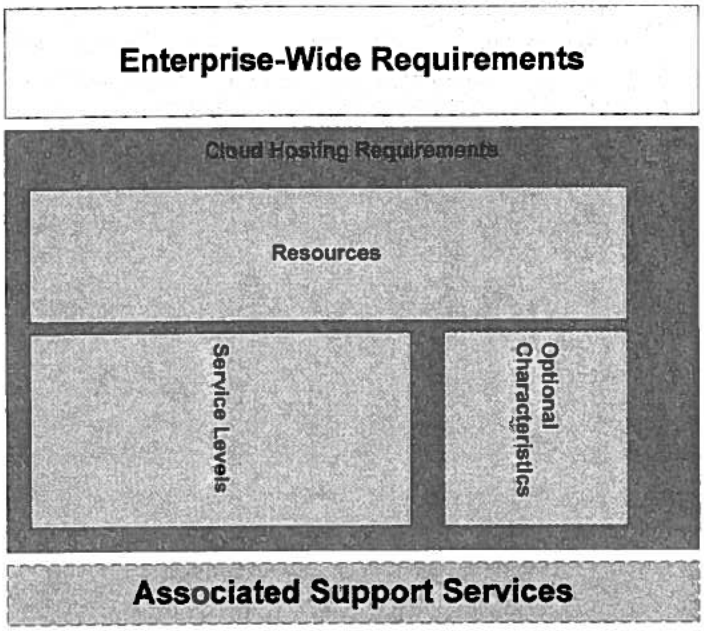


Figure 1 DOI IT Service Delivery Requirements

The Government shall retain ownership of any government designed/created/loaded data, policy, process, procedure, service template, workflow and application hosted on contractor's infrastructure, and maintains the right to request full copies of these at any time.

C.3.1 Enterprise-Wide Requirements

Enterprise-Wide Requirements are baseline requirements common to all dimensions of the service definition, and are applicable to all service lines. Regardless of the resources, service levels, optional characteristics, or additional services selected to fulfill a specific service requirement, all Enterprise-Wide Requirements must be met. Enterprise-Wide requirements are described in Section C.5, Establish and Meet Enterprise-wide Requirements.

C.3.2 Resources Requirements

Resource requirements describe the platform, infrastructure assets, and support required by an information system to operate as defined by SLA's and Operational Level Agreements (OLA's). Examples of platform resource requirements include Operating Systems, Databases, and other Middleware used. Examples of infrastructure resource requirements include "Compute Host" and Storage. The Resources dimension is more completely described in Section C.6, Establish and Meet Resource Requirements.

C.3.3 Service Level Requirements

Service Level requirements define the performance and other operating parameters within which the hosting services must operate to fulfill IT system and customer requirements. The Service

Level dimension is more completely described in Section C.7, Establish and Meet Portfolio of Service Level Requirements.

C.3.4 Optional Characteristics Requirements

Optional Characteristics define additional services that may be required by specific IT systems or hosting configurations that are not widespread enough to be considered a Resource or a Shared requirement. Examples of Optional Characteristics requirements include Forward Staging (including Content Delivery Networks and data application or telecommunications caching) and Operating System Patch Management. The Optional Characteristics dimension is more completely described in Section C.8, Optional Characteristics Requirements.

C.3.5 Associated Support Service Requirements

Associated support services are those services which may be required to enable identification, analysis, prioritization, preparation and migration of IT systems from the current operating environment to the target operating environment, or may be required to ensure sustained operations and maintenance of systems in the target operating environment. These Associated Support Services are more completely described in Section C.9, Associated Support Services.

C.3.6 Technical Service Definition Model Summary

The DOI objective is to design, procure and deliver technical services based upon the model described in this Section; therefore a "Technical Service" is defined as Resource or combination of Resources, provided at specified Service Levels, with specified Optional Characteristics, for a Fixed Price (FP) per unit of service. These Technical Services must be offered within the constraints of a common set of Enterprise-Wide requirements, and may require Associated Support Services. Individual Task Orders issued under this contract may define services and service lines through any combination of these service dimensions and/or technical service line definitions published in the DOI's "Mission-Facing" Service Catalog.

C.3.7 Cloud Definitions and Basic Cloud Requirements

The DOI acknowledges that the cloud services market is still developing, and that there are a variety of approaches to defining cloud services. The DOI recognizes the cloud service definitions and deployment models specified in National Institute of Standards and Technology (NIST) 800-145, "The NIST Definition of Cloud Computing". Service Models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The Cloud deployment models consist of Public, Private, Community, and Hybrid.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

Figure 2 NIST Cloud Computing Definition, below illustrates the NIST concept of Deployment Models, Essential Characteristics and Service Models for Cloud computing that the DOI has adopted.

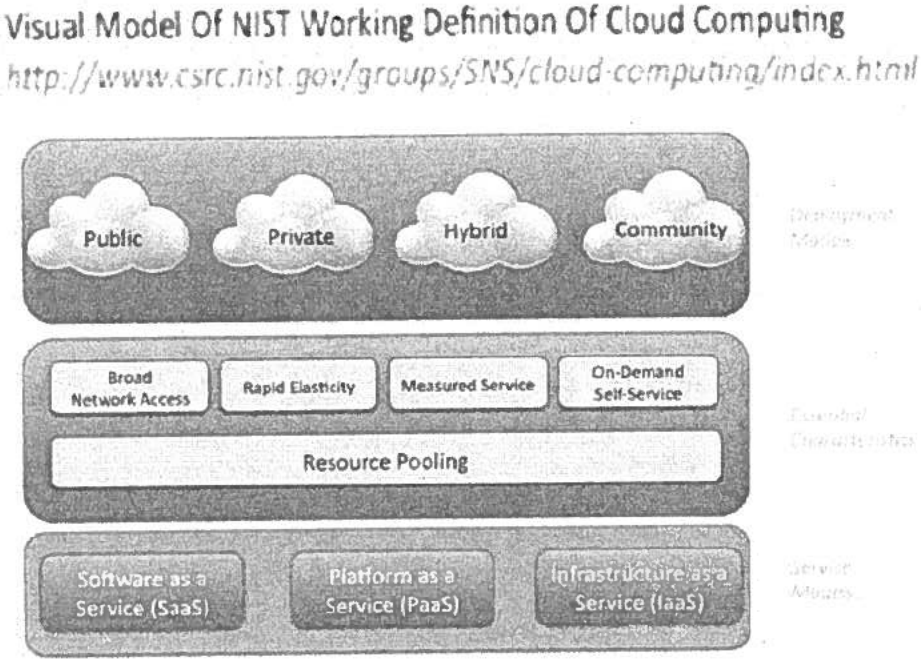


Figure 2 NIST Cloud Computing Definition

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

C.4 OVERVIEW OF CURRENT DOI OPERATING ENVIRONMENT

C.4.1 Organization

The U.S. Department of the Interior (DOI) is a Cabinet-level agency that manages America's vast natural and cultural resources. The DOI employs approximately 70,000 people, including expert scientists and resource-management professionals, in the nine technical bureaus, the federal shared service provider, and other supporting organizations listed below, herein after referred to as "Customer" organizations:

- Office of the Secretary (OS)
- Bureau of Indian Affairs (BIA)
- Bureau of Land Management (BLM)
- Bureau of Ocean Energy Management (BOEM)
- Bureau of Reclamation (BOR)
- Bureau of Safety and Environmental Enforcement (BSEE)
- National Business Center (NBC)
- National Park Service (NPS)
- Office of Surface Mining, Reclamation and Enforcement (OSM)
- U.S. Fish and Wildlife Service (FWS)
- U.S. Geological Survey (USGS)
- Other Interior Offices

There may be some organizational changes during execution of this contract, so the list above should not be considered definitive.

As part of the IT Transformation, the DOI is focused on an enterprise IT services model that will enable a unified strategy across the DOI and leverage a greater scale to drive more efficient operations.

C.4.2 Service Locations and End-points

DOI employees are located in over 2,400 offices in all 50 States, the District of Columbia, and U.S. Territories spanning 11 time zones. Approximately 80% of DOI employees work in locations with fewer than 25 total employees.

Many DOI employees and contractors regularly telework, travel or work for extended periods of time from remote field locations. Additionally, many DOI systems may need to be available to stakeholders in other government agencies and outside of the government domain.

C.4.3 IT Infrastructure Baseline

The DOI Bureaus and Offices currently deliver data and services from more than 400 locations. Over 30% of these locations and over 65% of DOI servers are located within one (1) hour driving distance of eight (8) metropolitan areas. The table below identifies key infrastructure metrics to support capacity analysis related to the current infrastructure.

Physical Servers	Storage Used (TB)	Racks	Gross Floor Area (sq. ft.)
~10k	>16k	>2,500	>300k

C.4.3.1 Data Centers

The DOI has applications and data distributed across over 400 datacenters, rooms, and closets throughout the United States.

Size (Gross Square Feet)	# Datacenters
<50	40
51-100	68
101-250	97
251-500	142
501-1,000	48
1,001 - 2,500	26
2,500- 5,000	16
>5,000	9

C.4.3.2 Data Center Access Channels

The DOI administers a Wide Area Network (WAN) that connects our internal customers, and provides the connection to external customers primarily via Trusted Internet Connection (TIC) sites. A number of remote sites may operate exclusively via dial-up circuits and satellite connections.

Additionally, the NBC, DOI's federal shared service center, currently provides virtual private networking services to more than 100 federal agency customers. These services are provided through Local Area Network (LAN), LAN-to-LAN Virtual Private Network (VPN) connectivity and Multi-Protocol Label Switching (MPLS)-dedicated circuits to both our hosting facilities and our Disaster Recovery (DR) sites.

Organizations within the DOI utilize a variety of WAN Optimization and application/desktop virtualization technologies to optimize utilization and available transport resources and meet end-user performance requirements.

C.4.3.3 Operating Systems

Operating System	% of Servers
Windows Server	63%
Unix Server	10%
Linux Server	17%
Other	10%

A more detailed description of operating systems in use can be found in Section C.6.1.1, Provide and Support Operating System Resource Requirements.

C.4.3.4 Enterprise Software Licenses

The DOI has a number of enterprise software licenses that are grouped into five (5) broad application classes:

1. Operating systems
2. Middleware (e.g., database managements systems)
3. Geographic Information System (GIS)
4. End-user productivity (e.g., collaboration)
5. Enterprise / mission applications (e.g., enterprise resource management, finance / HR, mission-specific)

A detailed description of the software in use is identified in 0 Establish and Meet Resources Requirements.

C.4.3.4.1 Categorization of Applications

The DOI's existing application environment presents a diverse set across a multitude of dimensions:

a. **Type:** Enterprise applications (e.g., Finance/HR), public facing web sites/applications, mission-specific applications;
b. **Software Source:** Commercial Off the Shelf (COTS), Government Off the Shelf (GOTS), DOI Custom, Aggregate Systems with DOI Developed Custom Interfaces.
c. **Security Categories:** Applications span the full range of security FIPS Pub-199 security categories for confidentiality, integrity and availability impact: "LOW," "MODERATE," and "HIGH";
d. **Hardware platform:** Applications cut primarily across Windows, Linux, and Unix, environments, with varying levels of modernization and customization;
e. **Application environments:** Application code base include varying levels of legacy and modern programming languages and customization; and
f. **Application Life-Cycle**: Steady State (Operations and Maintenance), Mixed State, and Development, Modification and Enhancement (DME).

C.4.3.4.2 Overview of Current Virtual Application Delivery Environment

The majority of applications reside upon corporate owned workstations. Several bureaus and offices within DOI have deployed existing Virtual Desktop and Application Delivery systems and a range of the solutions including but not limited to those listed below:

- Citrix XenDesktop
- Citrix XenApp
- VMWare View
- VMWare ThinApp
- Microsoft (Remote Desktop Services)
- Microsoft App-V

The existing systems are localized within the individual bureaus and are not scaled to support an enterprise the size of the DOI. There are approximately 30 significant instances of these technologies with an approximate combined concurrent license count around 5000.

The current DOI end user workstation environment consists primarily of Dell and IBM laptops/desktops running the Microsoft Windows XP or Windows 7 Operating System. However, there are also a growing number of mobile devices such as the Apple iPad/iPhone and Android/Windows Mobile tablet devices. While there is a wide range of desktop applications deployed, the applications common across the department consist of Microsoft Office Pro (2007/2010), Adobe, and select enterprise applications. The most common web browser is Internet Explorer, but others are also in use.

C.5 ESTABLISH AND MEET ENTERPRISE-WIDE REQUIREMENTS

Enterprise-Wide Requirements are baseline requirements that are common to all dimensions of the service definition, and are applicable to all service lines. Regardless of resources, service levels, optional characteristics, or additional services selected to fulfill a specific service requirement, all Enterprise-Wide Requirements must be met.

C.5.1 Comply with Essential Cloud Service Requirements

The Contractor shall provide a Cloud Computing solution that aligns to the following "Essential Cloud Service Characteristics" as defined in the NIST Working Definitions as described in **Table 1 Essential Cloud Services Characteristics** below:

Table 1 Essential Cloud Service Characteristics

Cloud Characteristic	Definition	General Requirement
C.5.1.1 On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.	The Contractor shall provide the capability for the ordering activity to unilaterally (i.e. without contractor review or approval) provision services.
C.5.1.2. Ubiquitous network access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).	2a. The Contractor shall support internet bandwidth within minimum service requirements established herein. 2b. The Contractor shall have a minimum of two data center facilities at two different geographic locations in the Continental United States (CONUS), at least 250 miles apart, and all services acquired will be guaranteed to reside in CONUS, Alaska, Hawaii or US Territories.
C.5.1.3. Location independent resource pooling	The provider's computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.	The Contractor shall support scaling of resources based upon the minimum requirements described herein and specified within the individual Task Orders.
C.5.1.4. Rapid elasticity	Capabilities can be rapidly and elastically provisioned to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for provisioning often appear to be infinite and can be purchased in any quantity at any time.	The Contractor shall support service provisioning and de-provisioning times (scale up/down), making the service available within minimum prescribed times of provisioning request.
C.5.1.5. Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.	The Contractor shall offer visibility into service usage via dashboard or similar electronic means.

C.5.2 Manage Service Delivery and Maintain Business Relationships and Interconnections

C.5.2.1 Provide Browser-based Management Functionality

The Contractor shall provide browser-based consoles, dashboards, portals, or interfaces for providing extensive self-service capabilities including (but not limited to):

C.5.2.1.1 Define User Roles and support User Authorization Workflows

Access to the Web management functionality shall be controlled via configurable role profiles that support highly customizable access rights including, but not limited to:

A. Restricting access to each component of the console (e.g., restricting who can provision resources or view reports)
B. Defining access rights for accessible components (e.g., scope of access, read-only versus read-write access)
C. Administrator roles with the ability to create, modify, delete, and configure user accounts, profiles and permissions.
D. Administrator capability to create authorization workflows with resource provisioning approval capabilities.

C.5.2.1.2 Provision, Configure, and De-provision (release) Resources

Access to the Web management functionality shall permit Provisioning, Configuring and De-provisioning resources and should include, but not be limited to the following:

A. User-initiated provisioning of resources defined in Section C.6 "Resources", as needed, without requiring human interaction with service provider; and
B. Configuring automatic provisioning (where appropriate) as defined in Section C.7.1.2 "Demand Fluctuations"
C. Resources (limit to templates identified in individual Task Orders)
D. End-user devices (e.g., mobile devices such as smartphones)

C.5.2.1.3 Monitor Performance and Manage Alerts and Reporting

A. General health and availability;
B. SLA performance;
C. Security;
D. Resources;
E. Configuring alarms and alerts; and
F. Active Service Summary.

C.5.2.1.4 Monitor Resource Usage/Utilization and Provide Cost Metering/Controls

The general requirement under this section is to provide tools for ensuring that task order spending rates remain consistent with the funding levels and task durations. Additionally these tools should provide alerts as spending approaches 85% of contracted funding levels.

C.5.2.1.5 Manage Open and Resolved Incidents and Service Requests

The general requirement under this section is to provide integrated tools and context filtered reporting to enable transparent monitoring and reporting of government initiated, and government service impacting incidents and service requests. These management capabilities include, but are not limited to the following:

- Integrated system and subsystem status reporting and incident correlation to assess incident impact on multiple systems, services, programs and users, and to facilitate pro-active communication with end-users, organizations and programs. This would include indicating both planned and unplanned downtime;
- On-line reporting of performance against key performance indicators identified in Section C.7 Establish and Meet Portfolio of Service Level Requirements, including, but not limited to: Mean Time to Resolve/Fix (MTF), Mean Time to Respond/Acknowledge (MTA);
- Prioritized queue of Incidents and Service Requests by Severity, with expected MTA and MTF based upon demonstrated performance. Including ability for authorized government official ability to establish/revise priorities and expedite;
- Repository of Reason for Outage (RFO) and Duration of Outage (DOO) information to support trend analysis and continual improvement efforts;
- Correlation of Complaints to Incidents;
- Rejected and Dropped Calls;
- Charting for Incidents per Hour, Day, Week, and/or Month over selected time period; and
- Integration with E-mail Alerts for incident volumes exceeding preset thresholds.

C.5.2.2 Support DOI System Interfaces

The Contractor shall provide the ability to connect a vendor-hosted system to another system that is hosted either at the DOI or at any external provider or customer, unless otherwise stated in specific Task Orders.

C.5.2.3 Implement Transparent and Effective Performance Management

The Contractor shall adhere to policies encouraging compliance with Service Level Agreements ("SLAs") and other requirements (e.g., incentives, disincentives and Quality Assurance Plans).

The Contractor shall provide clear access and visibility to ongoing performance and resources usage including, but not limited to:

a. Provide role filtered self management tools to support billing, monitoring, and reporting on service management functions;
b. Provide visibility into usage metering using metrics and granularity appropriate to the type of service;
c. Provide a suite of reports, dashboards, and alarms to monitor and track operational and infrastructure performance (e.g., incidents, service usage, capacity, SLA adherence);
d. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means;
e. Provide the ability to filter and view usage and invoicing by: Technical Service Line, bureau (and sub-bureau), program, IT System, IT System type, IT System Life-Cycle, Security Level, and other elements which may be identified in individual Task Orders;
f. Provide access to all log files generated by the hosted application, associated middleware, operating system, and underlying virtual and physical infrastructure;
g. Provide online reporting metrics interface for all resource utilization including metrics such as: current utilization, historical average and peak for a user defined window of time;

Additional performance management may be required by individual Task Orders. Reports shall be available for a period of time defined by the Task Orders.

C.5.2.4 Implement Efficient, Effective and Formal Governance

The Contractor shall specify policies and processes governing the interaction between the Contractor and the DOI, to include the following use cases:

a. Incident Management;
b. Process for monitoring and enforcing SLAs;
c. Role-based Access and Provisioning Authorities and Workflows;
d. Impact Plan in the event of a merger, acquisition, or divestiture;
e. Process for adding, deleting, or changing requirements, technical service lines, service levels, resource templates and optional features;
f. Process for assessing, planning, and mutual approval for achieving compliance with emerging regulations or policies.

C.5.2.5 Protect Intellectual Property Rights

The Contractor shall ensure the protection of DOI intellectual property (IP) and data ownership rights and those of any licensors.

C.5.2.6 Prohibit and Actively Prevent Adware, Spam, and Remarketing of Information

The Contractor shall not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the DOI. The Contractor and/or their agents shall not resell nor otherwise redistribute information gained from its access to the DOI.

C.5.3 Establish and Maintain Security and Privacy

C.5.3.1 Comply with FedRAMP and DOI Information Security and Privacy Requirements

The Contractor shall comply with the security and privacy requirements summarized in this section and as identified in the following Section J attachments:

a. Section J, Attachment 1 - DOI Security Control Standards;
b. Section J, Attachment 2 - Foundation Cloud Hosting Services Information Technology Security and Privacy Requirements for U.S. Department of the Interior;
c. Section J, Attachment 3 - DOI Privacy Loss Mitigation Strategy (PLMS); and
d. Section J, Attachment 4 - Additional IT Security Information

The referenced attachments identify laws, rules, regulations, standards, technology limitations and other constraints that the Contract shall adhere to or work under.

The hosting environment provisioned by the service provider must demonstrate an appropriate level of security by meeting the requirements of the Federal Information Security and Management Act (FISMA) for moderate-impact systems, and related agency-specific policies. This includes a formal agency security authorization review covering security controls, continuous monitoring, and identification of risks. The agency must consider and accept the risks before Authority to Operate (ATO) will be granted. The service provider must qualify for ATO no later than 120 calendar days from the date of award. Moreover, the service provider must become compliant with Federal Risk and Authorization Management Program (FedRAMP) requirements within 120 calendar days of the date it becomes available, and must maintain compliance throughout the period of performance. The continuous monitoring provided must comply with the NIST Special Publication 800-137 framework and Department of Homeland Security (DHS) guidance.

C.5.3.2 Provide User Authentication and Secure Connections

The Contractor shall ensure seamless integration with the DOI Identity, Authorization and Access Management (IdAAM) solution enabling hosted systems to authenticate users as well as devices using those credentials without requiring additional solution credentials.

Range of authentication and secure connection solutions includes, but is not limited to:

a. Active Directory;
b. Lightweight Directory Access Protocol (LDAP);
c. Secure Socket Layer (SSL);
d. Secure Shell (SSH);
e. Kerberos;
f. RACF; and
g. HSPD-12/Token

C.5.3.3 Comply with Security Assurance Requirements

In addition to complying with the general security and privacy requirements referenced above, the Contractor shall develop a Security Assessment Plan and initially assess all applicable security controls, using an agreed upon independent third-party assessor, and provide security assessment results in a Security Assessment Report. The report shall include a characterization and articulation of known remaining risks in order to support the DOI Authorizing Official's (AO) Authority to operate (ATO). In accordance with the OMB memorandum entitled, Security Authorization of Information Systems in Cloud Computing Environments, issued on December 8, 2011, the DOI AO anticipates leveraging and accepting provisional authorizations granted by the FedRAMP Joint Authorization Board (JAB), to the extent available, in granting security authorizations and an accompanying authority to operate (ATO) for DOI use of the Contractor services. DOI does not necessarily anticipate leveraging authorizations granted independently by other individual agencies, but may opt to do so at its discretion.

C.5.3.4 Complete Third Party Assessment of Security Controls and Mitigate Weaknesses

Controls within the following security control families (as defined by NIST) must be assessed by a third party on behalf of the Contractor. Additionally, Contractors will be required to develop and implement a plan to mitigate any weaknesses related to these controls.

C.5.3.4.1 Implement and Maintain Access Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Access Control requirements listed in the Bidder's Security Questionnaire, Section J, Attachment 5 (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.2 Implement and Maintain Awareness and Training Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Awareness and Training requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.3 Implement and Maintain Audit and Accountability Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Audit and Accountability requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.4 Implement and Maintain Security Assessment and Authorization Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Security Assessment and Authorization requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements

C.5.3.4.5 Implement and Maintain Configuration Management Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Configuration Management requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.6 Implement and Maintain Contingency Planning Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Contingency Planning requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.7 Implement and Maintain Identification and Authentication Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Identification and Authentication requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements.

C.5.3.4.8 Implement and Maintain Incident Response Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Incident Response requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements.

C.5.3.4.9 Implement and Maintain Maintenance Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Maintenance requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.10 Implement and Maintain Media Protection Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Media Protection requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.11 Implement and Maintain Physical and Environmental Protection Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Physical and Environmental requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.12 Implement and Maintain Planning Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Planning requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.13 Implement and Maintain Personnel Security Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Personnel Security requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.14 Implement and Maintain Risk Assessment Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific Risk Assessment requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.15 Implement and Maintain System and Services Acquisition Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific System and Services Acquisition requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.16 Implement and Maintain System and Communications Protection Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific System and Communication Protection requirements listed in the attached Bidder's Security Questionnaire (which includes the required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.3.4.17 Implement and Maintain System and Information Integrity Controls

The Contractor shall demonstrate and maintain full compliance with each of the specific System and Information Integrity requirements listed in the attached Bidder's Security Questionnaire (which includes required FedRAMP baseline controls and DOI Mandatory Enhancements).

C.5.4 Ensure Portability of IT Systems and Facilitate Migration between Service Providers

The Contractor shall ensure portability of IT Systems and facilitate migration of data and systems to another hosting solution (e.g., with another Contractor or within the DOI).

C.6 ESTABLISH AND MEET RESOURCE REQUIREMENTS

Resource requirements describe the platform, infrastructure assets, and support required by an information system to operate as defined by SLA's and Operational Level Agreements (OLA's). **Figure 3 Additional Detail on Resources and Service Levels** below illustrates an example of how the resources and associated services align within the Cloud Service Models.

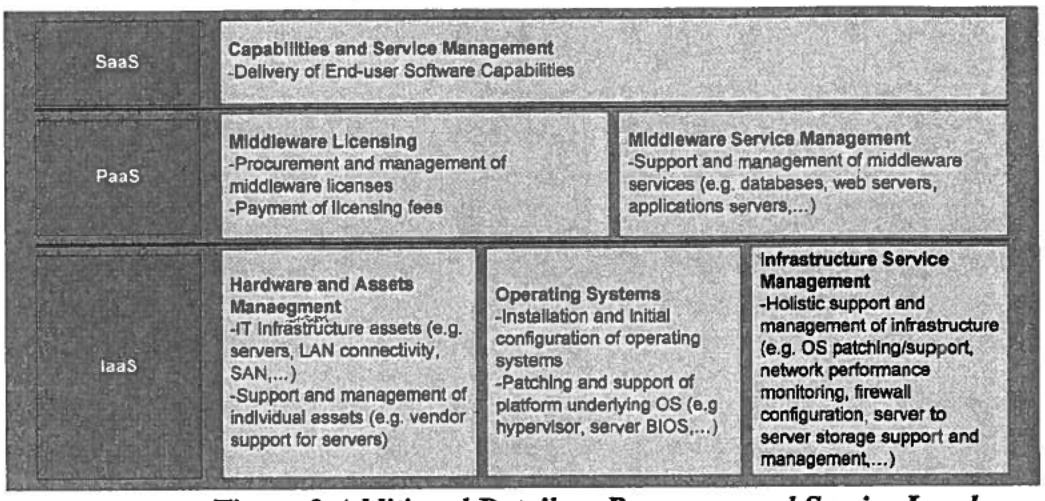


Figure 3 Additional Detail on Resources and Service Levels

Any requirements within this area will be specific in the individual Task Orders that may be required to address the resources outlined in this section along with the service level requirements addressed in Section.C.7, Establish and Meet Portfolio of Service Level Requirements.

C.6.1 Provide Basic Resources

C.6.1.1 Provide and Support Operating System Resource Requirements

The DOI operates an expansive set of operating systems across its various systems, which are outlined below. As described in the IaaS layer of Figure 4 Additional Detail on Resources and Service Levels, above, the DOI requires installation, configuration, patching, and support for the listed operating systems. There are several options for satisfying these requirements:

a. The Contractor shall provide the required services for directly supporting these operating systems;

b. The Contractor shall identify migration strategies and costs for transitioning to alternative operating systems, and provides the required services for the alternative operating system; and/or

c. The Contractor shall provide only infrastructure, as described in the IaaS layer, and leave the operating system installation, configuration, patching, and support to the DOI.

Regardless of the services provided by a vendor, the Department retains the option to install, configure, patch, and support custom operating system images on top of vendor or Department-managed infrastructure.

The DOI requires a process for providing access and support for current requirements and new operating systems and versions as they become available and/or the Department's needs evolve. Additionally, the DOI may establish range of versions for each operating system which must remain available to support the base of hosted IT systems, including versions which may no longer be supported by the manufacturer.

The Contractor shall support current installed base of Operating Systems, which includes, but is not limited to:

a. Windows Server: 2003 & 2008
b. Linux: Centos 5.7, Red Hat 5, Red Hat 6, Ubuntu, SUSE Enterprise 10, Scientific
c. Solaris 10 for SPARC
d. AIX

The Contractor shall also support timely upgrade to current versions of the above Operating Systems.

C.6.1.2 Provide and Support Compute-Host Resources

Provide access to, and support for, compute host instances in a variety of performance levels defined in terms of compute power, RAM. The DOI has defined a "core" as the compute power equivalent to a 2 Ghz processor, unless otherwise specified in individual task orders.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

In all options an equivalent solution of equal or better specifications will satisfy the requirement. The current installed base includes, but is not limited to those identified in Table 2 Minimum Compute-Host Configurations below:

Table 2 Minimum Compute-Host Configurations

	Minimum Configurations	
Standard	**Cores (#)**	**RAM (GB)**
Extra Small	1	2
Small	2	4
Medium	4	8
Large	8	16
Extra Large	16	16
High Memory		
Extra Small	1	4
Small	2	8
Medium	4	16
Large	8	32
Extra Large	16	64
High Compute		
Medium	4	2
Large	8	4
Extra Large	16	8
High Compute Cluster		
Large	32	32
Extra Large	64	64
Custom		
(Task Order Defined)	TBD	TBD

C.6.1.3 Provide and Support Storage Resources

The Contractor shall provide the ability to provision storage services in a variety of performance classes, tiers, and/or pools. Performance classes shall be distinguished by the throughput supported by each class. The latency of storage accesses for all classes shall be in line with industry standards.

The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the authorized users via Internet through a web browser.

All storage facilities that store Federal Records must meet NARA 1571 Archival Storage Standards (http://www.archives.gov/foia/directives/nara1571.pdf).

C.6.1.3.1 Identify and Provide Access to Storage APIs

The Contractor shall identify Application Programming Interfaces (APIs) required to access and manage storage.

C.6.1.3.2 Support Storage of Both Files and Data Objects

The Storage Services shall support storage of both files and storage of data objects.

C.6.1.3.3 Support Standard Storage Operations

The Storage Services shall support the operations identified in Table 3 Command/Request Definitions below.

Table 3 Command/Request Definitions

Request/Operation	Container/Bucket	Object/File
PUT	PUT operations performed against Container/Bucket are used to create that container.	PUT operations against an Object are used add object to the bucket/container and write, overwrite, an object's metadata and content.
GET	GET operations performed against Container/Bucket lists information about objects within that container/bucket.	GET operations against an Object are used to retrieve objects and the objects' data from the container/bucket.
HEAD	HEAD operations against a storage Container are used to determine the number of Objects, and the total bytes of all Objects stored in the Container.	HEAD operations against an Object are used to retrieve object's metadata and other HTTP headers.
DELETE	DELETE operations performed against Container/Bucket deletes the container/bucket.	DELETE operations against an Object are used to permanently delete the specified object.
POST POST is an alternate form of PUT that enables browser-based uploads	The POST request operation adds an object to a container/bucket using HTML forms.	POST operations against an Object name are used to set and overwrite arbitrary key/value metadata.
COPY	The COPY operation creates a new, uniquely named copy of a container/bucket that is already stored.	The COPY operation creates a uniquely name copy of an object/file that is already stored.
LIST	The LIST operation displays the information of a current Container/Bucket.	The LIST operation displays the current objects/files, including metadata.

C.6.1.3.4 Support Storage Resource Classes

For each Class proposed by the Offeror, a solution of equal or better specifications than identified in **Table 4 Proposed Storage Class** below will satisfy the requirement.

Table 4 Proposed Storage Class

Storage Class	Throughput	Uptime/ Availability	Example
A	8 Gbps	100%	high-speed SAN
B	1 Gbps	100%	low-speed SAN
C	50 Mbps	99.90%	Remote On-line Storage
D	Access within 24 hrs	offline	Tape Library

Independent Task Orders may specify selected storage class and availability requirements and may also specify that Class C and Class D storage be stored in a facility other than the one hosting the related mission system.

***C.6.1.3.5* Support Data Migration Across Storage Classes**

The Contractor shall provide support for migrating data across different classes. This support shall include a web-based interface for manually migrating data across different tiers as well as an open source API interface for accessing the same functionality.

***C.6.1.3.6* Support Alternative Backup Solutions**

The DOI requires the ability to design and manage backup solutions, and/or to utilize offeror-provided backup solutions.

The Contractor shall provide backup at both onsite and offsite locations, and may provide software solutions to manage the backup processes.

The Contractor shall ensure that all Archive and Backup services meet all of the requirements described in Section C.5.3, Establish and Maintain Security and Privacy.

The Contractor shall ensure the Web-management functionality includes:

a. Ability to configure backup schedule;
b. Ability to restore files and images from backup;
c. Ability to configure a retention period and automatic deletions of old files;
d. Ability for government to specify the level of redundancy required; and
e. A scripting interface for the above.

C.6.1.3.7 Support Secure Transfer of Physical Media

When transferring physical media between locations, the Contractor shall provide a certified courier or other method of maintaining a secure chain of custody over tapes and other media being moved to and from a defined, secured off-site storage location. The Contractor shall provide flexibility in courier pick-up and delivery time.

C.6.1.4 Provide Transport Resources and Support Interconnections

C.6.1.4.1 Comply with General Transport Requirements

The DOI requires access to transport resources that meet the following requirements:

- **a.** The bandwidth consumed by each system shall be calculated using a 95th percentile method, with samples taken at a minimum of every five (5) minutes or less. The Contractor shall specify proposed range of sample rates within this range.
- **b.** Each system shall have access to sufficient bandwidth to meet its monthly data transfer needs as established in individual Task Orders.

C.6.1.4.2 Comply with Interconnection Configurations and Requirements

The Contractor shall support access to network connectivity in the following configurations:

- **a.** Between compute host instances;
- **b.** Between vendor datacenters;
- **c.** Between a vendor datacenter and the Department intranet;
- **d.** Between vendor datacenters and the internet; and
- **e.** Between vendor datacenters and DOI customers, including LAN-to-LAN VPN connectivity and dedicated circuits (e.g., T-1, DS-3, etc.).

C.6.2 Provide Aggregated Resources and Enabling Services

Aggregated Resource Services are combinations, or packages, of basic resources, (Operating System, Compute-Host, Storage, Telecommunications/Networking, Middleware, Scripting, and Programming).

Enabling Services describe reusable processes and activities that support multiple technical services. Additional Aggregated Resource Services and Enabling Services may be defined by the Contractor or by the DOI within individual Task Orders to facilitate communication, streamline ordering or provisioning, or simplify definition and pricing for higher order or advanced Services. Aggregated Resource Services and Enabling Services are high order components for defining Technical Services and Technical Service Lines delivered under the anticipated contract.

C.6.2.1 Provide Aggregated Resource Services

C.6.2.1.1 Provide Secure File Transfer Resources

The Contractor shall provide a Secure File Transfer solution that satisfies the requirements in Section J, Attachment 12, Secure File Transfer Requirements.

C.6.2.1.2 Provide Virtual Machine Resources

The service shall be available online, on-demand and dynamically scalable up or down per request for service from the end users via Internet through a web browser. **Table 5 Virtual Machine Service Requirements**, below provides a description of the general service and Resource requirements for Virtual Machines.

Table 5 Virtual Machine Service Requirements

Aggregate Resource Description	Resources
Virtual Machines- • Service shall provide scalable, redundant, dynamic computing capabilities or virtual machines. • Service shall allow Government users to procure and provision computing services or virtual machine instances online via the Internet. • Service shall allow users to remotely load applications and data onto the computing or virtual machine instance from the Internet. • Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the Internet.	**Compute-Host Resources** **CPU (Central Processing Unit)** - CPU options shall be provided as follows: • A minimum equivalent CPU processor speed of 2GHz shall be provided. Additional options for CPU Processor Speed may be provided, however it is not required. • The CPU shall support 32-bit or 64-bit operations . **RAM (Random Access Memory)**: Physical memory (RAM) reserved for virtual machine instance or Computing supporting a minimum of 1GB of RAM. **Operating System (OS) Resources** Service shall support at least the following OS: Windows, Unix, LINUX, or Solaris (Intel or SPARC). **Storage Resources** Disk Space options allocated for all virtual machines and file data supporting the minimum bundled storage. **Transport Resources**: Transport resources utilized to transfer data in/out of the provider's infrastructure supporting the minimum data requirements. If there are costs associated with data transfer over and above ordinary transport charges, or there are special capabilities for bulk transfer, please indicate clearly in Section B pricing tables.

Table 6 Virtual Machine Block Storage Service Requirements below provides a description of the general service and resource requirements for Virtual Machine Block Storage.

Table 6 Virtual Machine Block Storage Service Requirements

Service Description	Resources
Disk/Block Storage Service – • Service shall provide scalable, redundant, dynamic Web-based storage. • Service shall provide users with the ability to procure and provision block storage capabilities for cloud virtual machines remotely via the Internet. • Service shall provide block storage capabilities on-demand, dynamically scalable per request for virtual machine instances.	• **Block Storage** –Once mounted, the block storage should appear to the virtual machine like any other disk.

The Government retains ownership of all virtual machines, templates, clones, and scripts/applications created with individual task orders issued under this contract as well as maintaining the right to request full copies of these virtual machines at any time.

The Government retains ownership of customer loaded software installed on virtual machines and any application or product that is developed under orders against this contract.

The Contractor shall:

1. Provide virtualization services for the customer to be able to spawn on-demand virtual server instances.
2. Support a secure administration interface, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH), for the Government designated personnel to remotely administer their virtual instance.
3. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption.
4. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing.
5. Provide multiple processor virtual machines.
6. Manage processor isolation in a multi-tenant environment.
7. Provide capability to perform live migrations (ability to move running VM's) from one host to another.
8. Provide a hypervisor which supports security features such as role-based access controls and auditing of administrative actions.
9. Provide a hypervisor which supports hardware-assisted memory virtualization.

C.6.2.1.3 Provide Database Hosting Resources

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Suppo t Current Range of Database software, which includes, but is not limited to:

a. Informix
b. MS SQL Express
c. MS SQL Server (2005, 2008, 2010, 2012)
d. MySQL
e. Oracle 10g
f. Oracle 11g
g. Oracle 8a
h. PostGIS
i. PostGreSQL
j. SQLite
k. Sybase IQ

The Contractor shall also support timely upgrade to current versions of the above database software.

The Contractor shall support additional database software as specified individual Task Orders.

C.6.2.1.4 Provide Web Hosting Resources

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support Current range of Web Server software, which includes, but is not limited to:

a. Apache
b. TomCat
c. Jeronimo
d. IBM WebSphere
e. ORACLE Application Server
f. JRUN
g. Glass Fish
h. IBM HTTP Server
i. IIS
j. Jetty (Eclipse Foundation)

Contractor shall also support timely upgrade to current versions of the above Web Hosting Resources.

Contractor shall support additional Web Hosting Resources as specified in individual Task Orders.

C.6.2.1.5 Provide Development and Test Environment

The Contractor shall provide support for non-production environments with a range of instances of technical service lines. These non-production environments are characterized by different controls, boundaries and levels of access, which may be specified in the individual Task Orders.

C.6.2.1.6 Provide Application Hosting

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support the current range of Application Server software, which includes, but is not limited to:

a. Cold Fusion
b. Glass Fish
c. Hibernate
d. JBOSSApp Server and Suite
e. Matlab
f. MediaWiki
g. Oracle Application Server and BPM Middleware
h. Silverlight
i. Sun SMQ
j. Tuxedo
k. WebLogic
l. WordPress

Contractor shall also support timely upgrade to current versions of the above Applications. Contractor shall support additional Applications as specified in individual Task Orders.

C.6.2.2 Provide Enabling Services

C.6.2.2.1 Support Bulk Data Transfer and Provide Competitive Volume Discounts

The Contractor shall provide volume pricing, for periodically transferring large amounts of data into or out of the Contractor-hosted environment, and between sites within the Contractor environment. These transfers may originate or terminate at both DOI and non-DOI facilities (e.g., universities). The volume of data transferred could range from the size of virtual machine images to all of the DOI data stored in the Contractor environment.

The Contractor shall support the following modes for Bulk Data Transfer:

a. Loading data from physical media (e.g., disk arrays, tapes, DVDs)
b. Transferring data in/out over the Internet
c. Transferring data in/out to the DOI intranet
d. Transferring data in/out via dedicated circuits (including virtual private networks).

C.6.2.2.2 Provide Operating System Services

The DOI requires several operating system services. All services can be performed by either the Contractor or the DOI, but the DOI retains the right to perform any service itself. These services include configuring Operating Systems and troubleshooting Operating System Problems.

C.6.2.2.3 Provide Licensing and Installation Services

The DOI requires the licensing and installation of all necessary operating systems and software that is the Contractor responsibility under service or service line bundles.

C.6.2.2.4 Provide Patching and Version Control Services

The Contractor must commit to a defined patching schedule and process (e.g., the DOI shall be notified in advance and given sufficient time to test compatibility with all related software – example time for implementation could range from a few days to a few weeks after identification).

The Contractor shall comply with negotiated change control processes and authorities for change, as mutually agreed upon after award. The Contractor shall coordinate with the system owner prior to making changes to the hardware configuration that may also require changes to the business system.

All proposed modifications shall be documented, tested, planned and communicated to client to ensure compatibility with the business system and to include fall back procedures. The Contractor shall provide the DOI at least one (1) week to test patches before they are rolled out to production systems. The DOI may postpone the patch indefinitely for selected environments if it is unable to make deployed IT systems compatible with the new versions.

The Contractor shall cooperate with the DOI to establish recurring maintenance windows and limit all but critical security patches to distribution within these windows.

C.6.2.2.5 Provide Disaster Recovery Services

For all Disaster Recovery the Contractor shall provide the following services:

A. Support to design, implement, and manage the Disaster Recovery solution

B. Provide a web-based capability for configuring Disaster Recovery options.
- ***I.*** Establish a set of mission critical data and snapshots.
- ***II.*** Provide all services required in order to execute failover in the event of disaster and bring mission critical systems and data online.

C.6.2.2.6 Support One or More Solutions for Middleware Licensing and Support

The DOI operates an expansive set of middleware platforms across its various systems, which support Web Hosting, GIS, Database and Applications. The DOI requires licensing and management services for all middleware platforms identified herein. There are several options for satisfying these requirements:

A. *Contractor Provided Licensing and Management for Current Portfolio.* The contractor shall provide the licensing and/or management services for directly supporting current portfolio of DOI platforms and additional platforms as may be identified in individual Task Orders; and/or

B. *Contractor Proposed Migration to Recommended Standard.* The Contractor shall identify migration strategies and costs for transitioning to an alternative platform, and provides the licensing and/or management services for the alternative platform; and/or

C. *DOI Provides Licensing and Management.* The Contractor shall provide only infrastructure, as described in the IaaS layer, and DOI shall manage and license middleware.

Regardless of the services provided, the DOI retains the option to install, manage, and provide its own support for middleware instances on top of Contractor or DOI-managed infrastructure.

C.6.2.2.7 Provide Hosting for DOI Legacy Metering and Reporting Software. However, the following information should be considered a sampling of the current environment. Support the current range of Metering and Reporting software, which includes, but is not limited to:

a. Actuate
b. AWStats
c. Crystal Reports
d. Fiddler
e. Groundworks
f. Hyperion SQR
g. IBM Applications Service Center
h. Jasper Server
i. MS SCOM
j. NAGIOS
k. SmarterStats
l. Splunk
m. Windows Log Parser

Contractor shall also support timely upgrade to current versions of the above legacy metering and reporting software. Contractor shall support additional metering and reporting software as specified in individual Task Orders.

C.6.2.2.8 Provide Hosting for Other Middleware

Specific Certification Requirements will be identified in the individual Task Orders. However, the following information should be considered a sampling of the current environment. Support the current range of Other Middleware, which includes, but is not limited to:

a. Atlassian JIRA
b. Adobe Pro
c. ArborText
d. Citrix XenApp
e. Citrix XenDesktop
f. Citrix XenServer
g. Common Spot
h. CommVault
i. Documentum
j. Exlips Plut-ins
k. Entellitrak
l. Hydra
m. IBM FileNet
n. Microsoft Dynamix CRM 2011
o. Net Backup
p. Networker
q. Oracle ADF
r. Prolifics
s. PureDisk
t. SharePoint
u. Software AG/Entirex DCOM (Communicator, XML Mediator, Adapters)
v. SQL Forms
w. Web Center Content
x. XML Data Powers

Contractor shall also support timely upgrade to current versions of the above Middleware. Contractor shall support additional Middleware as specified in individual Task Orders.

C.6.2.2.9 Provide Hosting for Scripting and Programming Environments

The DOI requires access to the following scripting languages on all web and application servers.

a. .NET
b. ASP.net
c. Flex Action Script
d. ISAPI
e. Java
f. Java Script
g. Jscript
h. Node.js
i. 4GL
j. Perl

k. PHP
l. Python
m. RScript
n. Ruby on Rails
o. UNIX Scripting

Contractor shall also support timely upgrade to current versions of the above scripting and programming environments. Contractor shall support additional scripting and programming environments as specified in individual Task Orders.

C.6.2.2.10 Provide or Support Virtual Application and Virtual Desktop Resources

A. Support Virtual Application/Desktop Capabilities-

The DOI desires to meet the following Application/Desktop Virtualization Goals:

- The ability for our users to leverage any device, anywhere, at any time, with the appropriate level of information assurance.
- The ability to equip users quickly with necessary tools, improve customer service, and lower costs.
- An enterprise-class virtual desktop/application solution that may scale to service all government employees within the scope of the task order award.

B. Support General Virtual Application/Desktop Capabilities

Table 7 Virtual Application and Desktop User Needs below, identifies a representative list of DOI user requirements for virtual applications and desktops.

Table 7 Virtual Application and Desktop User Needs

User Needs
The ability to work from home and on "Personally Owned Equipment" (POE), even when using computationally intensive tasks.
The ability to work in other DOI facilities and Federal, State and Local Partners (public, private and non-profit).
The ability to share large amounts of data with external partners at their locations.
The ability to collect information while in field locations with no connectivity and upload the information without having to come into the office (via from home or other locations with cellular, WI-FI, or wired connection to the Internet).
The ability to collect and analyze data while in the field or on travel, accomplish office work, and use the same device for possible non-business purposes due to weight or space restrictions.
The ability for remote access to DOI information using mobile devices without smart card readers
The ability for authorized government users to specify custom desktop images which include a wide range of applications, and deploy these images within timelines which may be identified in the individual task orders.
The ability to conduct self-service password reset from outside the network.

C. Support Additional Virtual Application/Virtual Desktop Requirements

Virtual Application and Virtual Desktop solutions should satisfy user requirements, use cases and other requirements identified in the individual task orders.

C.7 ESTABLISH AND MEET PORTFOLIO OF SERVICE LEVEL REQUIREMENTS

Service Level requirements define the performance and other operating parameters within which the infrastructure must operate to meet IT System and End User requirements. For this section "Days" refer to calendar days unless an alternative definition is explicitly provided for a specific service level metric in individual task orders.

C.7.1 Optimize End-to-End Performance

C.7.1.1 Manage Latency between Hosted Applications and End Users

Latency shall be managed, by the Contractor, so as to optimize IT System responsiveness to end users and ensure functionality of the hosted application. The Contractor shall cooperate with the DOI to configure and maintain system infrastructure elements to ensure end-to-end latency is in compliance with IT system and end-user service level commitments. The assumption of both parties during the evaluation and resolution of end-to-end latency issues shall be that there is joint responsibility, and only upon identification of the latency issue(s) shall final responsibility be assigned. Additionally, the Contractor shall provide or cooperate with the DOI to deploy Virtual Application Hosting to improve user experience. Specific latency requirements, if any, will be identified in individual task orders.

C.7.1.2 Adapt to Demand Fluctuations to Meet and Maintain Service Levels

The Contractor shall ensure that system infrastructure is able to accommodate fluctuations in demand with minimal impact on system performance. Anticipated seasonality, minimum, peak and average demand rates will be provided in individual task orders to facilitate resource planning. Individual Task Orders may identify selected methods and minimum times for adapting to demand fluctuations.

C.7.1.3 Streamline and/or Automate Resource Scaling

The Contractor shall provide several tiers of service for the scale of basic resources that must be readily provisionable at all times. The Contractor shall provide capability to template incremental tiers for each resource or service package. Alternative methods for meeting the objective to streamline incremental provisioning for common, cost effective configurations based upon appropriate combinations to scale based upon application Input-Output (I/O), Processor, Memory or Storage sensitivity will also be considered. The DOI approved tiers/templates shall be selectable within the provisioning portal, and authorized users shall be able to establish the resource scaling sequence most appropriate to their application when configuring automatic scaling. Minimum timelines for implementing scaling options may be identified in individual Task Orders.

C.7.2 Meet Software and Licensing Support Service Level Requirements

C.7.2.1 Meet Operating System Services Service Level Requirements

Specific Service Levels for Operating Systems may be identified in the in individual Task Orders.

C.7.2.2 Meet Licensing and Installation Services Service Level Requirements.

Specific Service Levels for Licensing and Installation may be identified in the individual Task Orders.

C.7.2.3 Meet Patching and Version Control Services Service Level Requirements.

Specific Patching and Version Control Service Levels may be identified in the individual task orders.

C.7.3 Meet Uptime and Availability Requirements

The Contractor shall guarantee several tiers of uptime of all Contractor controlled resources in terms of percentage of minutes a month that the Contractor controlled resources shall be fully operational and available. Planned downtime, as defined in **Table 17 Scheduled Downtime Service Bands**, Meet Mean-Time-To- Restore Service Levels, is counted as the system being fully operational. **Table 8 Uptime and Availability Service Bands** below identifies the minimum performance levels required for uptime and proposes options for up to four (4) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to four (4) alternative service bands.

Table 8 Uptime and Availability Service Bands

Uptime

Service Band	Minimum (>=)	Maximum (<)	Maximum Planned Downtime
Band 1	99.99%	100%	<4 min/month
Band 2	99.90%	99.99%	<43 min/month
Band 3	99%	99.90%	<7.2 hours/month
Band 4	95%	99%	<36 hours/month
Minimum Acceptable Performance:	95%		<36 hours/month

C.7.4 Meet Disaster Recovery Services Service Levels

The DOI requires a Disaster Recovery plan that meets all requirements outlined herein, and Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified below and in the individual task orders. Additional, Specific Disaster Recovery Service levels may be identified in the individual task orders.

C.7.4.1 Meet Recovery Time Objectives (RTO)

The Contractor shall guarantee that, following any outage attributable to failure of the infrastructure support, systems will be made operational within a specified maximum time. The table below identifies the minimum performance level for RTO and proposes options for up to five (5) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to five (5) alternative service bands.

Table 9 Recovery Time Objective Service Band Recommendations

Recovery Time Objective (RTO)		
Service Band	**From**	**To**
Band 1	0 minutes	5 minutes
Band 2	5 minutes	4 hours
Band 3	4 hours	24 hours
Band 4	24 hours	48 hours
Band 5	48 Hours	7 Days
Minimum Acceptable Performance:		7 Days

C.7.4.2 Meet Recovery Point Objectives (RPO)

The Contractor shall guarantee that, following a triggering event, systems will be reverted to a prior state no older than the specified maximum duration. Table 10 Recover Point Objectives below identifies the minimum performance level for RPO and proposes options for up to five (5) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to five (5) alternative service bands.

Table 10 Recover Point Objectives

Recovery Point Objective (RPO)		
Service Band	**From**	**To**
Band 1	0 minutes	5 minutes
Band 2	5 minutes	4 hours
Band 3	4 hours	24 hours
Band 4	24 hours	48 hours
Band 5	48 Hours	7 Days
Minimum Acceptable Performance:		7 Days

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

C.7.5 Meet Backup Service Levels

The following service level requirements apply to Backup Services.

C.7.5.1 Comply with Backup Frequency Requirements

The Contractor shall provide a means of configuring backup and archiving frequency on an authorized technical user defined schedule. The schedule shall support daily, weekly, monthly, and yearly backups. The DOI authorized technical user shall be able to select a different Mean Time to Restore and Retention Periods for each backup. Specific Backup Frequency requirements may be identified in the individual Task Orders.

An example backup schedule could be:

Table 11 Recommended Backup Service Levels and Retention Periods

Backup Service Levels

Frequency	Retention Period	Mean-Time to Restore
Daily	2 weeks	15 minutes
Weekly	1 month	4 hours
Monthly	1 year	24 hours
Yearly	48 Hours	72 hours

C.7.5.2 Meet Mean Time to Restore Requirements.

The average time required to complete a restore request. Given that the size of a restore request will influence time required to restore it, these service levels are calculated as the average of all restore requests (both big and small) over a month. Specific Mean-Time to Restore requirements may be identified in the individual Task Orders.

Table 12 Mean Time to Restore Requirements

Backup Service Levels

Service Band	Mean-Time to Restore
Band 1	15 minutes
Band 2	4 hours
Band 3	24 hours
Band 4	72 hours

C.7.5.3 Comply with Data Retention Policies

The retention period is the duration that each backup snapshot will be retained before automatic deletion. The DOI requires the ability to set a custom time period within individual Task Orders.

C.7.6 Document and Meet Provisioning Service Level Requirements

The Contractor shall provide several tiers of service for the speed in which a hosted system can respond to changes in demand. In all cases resources shall be brought online and available for use within the specified time as defined within the individual task orders.

For example, in order to retain flexibility to scale up resources quickly to respond to sudden spikes in demand, some systems may subscribe to a top tier. Other systems, though, with more predictable changes in demand may be able to plan further ahead and subscribe to lower tiers of service.

After a request has been made (either manually or automatically in response to configurable triggers), resources (e.g., storage, virtual machines) shall be available for use within the specified times.

C.7.6.1 Meet Compute Host and Operations System Provisioning Service Level Requirements

The Contractor shall provide a means to provision the Compute Host manually, and/or scale Compute Host Resources both manually and automatically. The Table 13 Compute Host Service Bands below identifies the minimum performance level and proposes options for up to four (4) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to four (4) alternative service bands. Time measurement assumes that the user possess appropriate provisioning authorization credentials.

Table 13 Compute Host Service Bands

Service Band	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min
Band 2	15 min	2 hours
Band 3	2 hours	8 hours
Band 4	8 hours	24 hours
Minimum Acceptable Performance:		24 hours

C.7.6.2 Meet Storage Provisioning Service Level Requirements

The Contractor shall provide a means to provision the Storage both manually, and/or scale Storage Resources both manually and automatically. The table below identifies the minimum performance level and proposes options for up to four (4) service bands. The Contractor shall meet the minimum performance requirement, but may propose one (1) to four (4) alternative service bands. Time measurement assumes that the user possess appropriate provisioning authorization credentials. Table 14 Storage Provisioning Service Bands identifies proposed Service Bands for Provisioning Storage.

Table 14 Storage Provisioning Service Bands

Service Band	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min
Band 2	15 min	2 hours
Band 3	2 hours	8 hours
Band 4	8 hours	24 hours
Minimum Acceptable Performance:		24 hours

C.7.7 Meet Middleware Management Service Level Requirements

The Contractor shall provide several tiers of management support for Database, Web Server, and Application Servers. These services shall include the following requirements:

C.7.7.1 Meet Middleware Patching and Version Control Requirements

The Contractor shall commit to a defined patching schedule and process (e.g., the DOI must be notified in advance and given sufficient time to test compatibility with all related software – example time could range from a few days to a few weeks, and could postpone the patch indefinitely if it could not be made compatible). This section also defines any requirements around how quickly the Contractor shall make new versions of any support software available for use.

The Contractor shall provide the DOI test patches at least 1 week before they are rolled out to production systems.

The Contractor shall ensure all proposed modifications are documented, tested, planned and communicated to consumer to ensure compatibility with the business system and to include fall back procedures.

The Contractor shall coordinate with the system owner prior to making changes to the hardware configuration that may also require changes to the business system.

Required Schedules:

a. Weekly
b. Monthly
c. Quarterly
d. Yearly

C.7.7.2 Meet Additional Middleware Service Level Requirements

The Contractor shall meet additional middleware service level requirements which may be identified in the individual Task Orders.

C.7.8 Meet SAP Hosting Performance Requirements

The Contractor shall provide several tiers of service for SAP Hosting Services. The Contractor shall retain flexibility in how performance metrics are met, but shall guarantee service levels established in the individual Task Orders

C.7.8.1 Meet SAP Computation Performance Requirements

The Contractor shall provide SAP configurations with scalable processing performance. Total performance of the configuration must be scalable up and down to meet requirements from 20,000 SAPS (or equivalent) up to and including 1,800,000 SAPS (or equivalent) As performance needs grow it must be possible to scale performance up even further; anticipated performance objectives for FY2019 are expected to be 2,500,000 SAPS (or equivalent).

C.7.8.2 Meet SAP RAM Performance Requirements

The Contractor shall provide SAP configurations with scalable RAM availability. Total RAM available to the configuration must be scalable up and down to meet requirements from 800GB up to 13,000 GB. As RAM needs grow it must be possible to scale RAM up even further; anticipated RAM requirements for FY2019 are expected to be 17,000 GB.

C.7.8.3 Meet SAP Storage Performance Requirements

The Contractor shall provide SAP configurations with scalable storage availability. Total storage available to the configuration must be scalable up and down to meet requirements from 3.5TB up to 600TB. As storage needs grow it must be possible to scale storage up even further; anticipated storage requirements for FY2019 are expected to be 1,900 TB.

C.7.8.4 Meet Additional SAP Performance Metric Requirement

Additional Performance metrics related to SAP Application Hosting shall be identified in the individual Task Orders for those services.

C.7.9 Meet Secure File Transfer Service Levels

Specific service level requirements for the Secure File Transfer technical service line will be identified in the individual task orders. Section J, Attachment 12 identifies the initial requirements for this technical service.

C.7.10 Meet Virtual Desktop and Applications Service Levels

Specific service level requirements for Virtual Desktop and Applications Services will be identified in the individual Task Orders.

C.7.11 Meet Customer and Program Support Service Levels

The DOI requires several tiers of support for any support services provided. Support services include both trouble ticket support, as well as service management (e.g., Infrastructure Service Management, Operating System Service Management, and Middleware Service Management).

For each tier of support, the DOI requires pre-defined service levels for the following metrics:

a. Availability (defined in section C.7.11.1 Meet Service Center Availability Service Levels)
b. Time to Respond (defined in section C.7.11.2 Meet Service Level Time To Respond (Acknowledge) to Requests Service Levels)
c. Time to Resolve (defined in section C.7.11.3 Meet Mean-Time-To-Resolve Service Levels)

Planned downtime (defined in Table 19 in section C.7.11.4

d. Minimize Planned Downtime and Maintenance Windows)

The DOI requires the following definition of support and service request severity:

a. Severity 1: Emergency (Health and Safety)
b. Severity 2: Mission Priority (Bureau Director)
c. Severity 3: Program Priority
d. Severity 4: Routine

In addition, within thirty (30) calendar days of any major outage occurrence resulting in greater than 1-hour of unscheduled downtime, the Contractor shall describe the outage including description of root-cause and fix.

C.7.11.1 Meet Service Center Availability Service Levels

During hours of availability the customer expects to reach a support or service person who is able to take down a request for service or log a trouble ticket. Specific Service Center Availability Service Levels will be selected from the available tiers in the individual task orders.

The DOI requires the following tiers of availability:

C.7.11.1.1 8x5 Single Time zone

- 9am to 5pm
- Monday through Friday
- in a single time zone which may be identified in the individual task orders

C.7.11.1.2 8x5 CONUS

- 9am to 5pm
- Monday through Friday
- in each of the 4 CONUS Time zones (Eastern, Central, Mountain, and Pacific)

C.7.11.1.3 8x5 CONUS + Alaska

- 9am to 5pm
- Monday through Friday
- in each of the 4 CONUS Time zones (Eastern, Central, Mountain, and Pacific) plus Alaska

C.7.11.1.4 24x7x365/366

- 24 hours a day
- 7 days a week

C.7.11.1.5 Custom Work Hours, Custom Work Week, Selected Time Zone(s)

- To be defined in individual Task Orders.

C.7.11.1.6 Defined Season or Emergency/Incident Support

- To be defined in individual Task Orders.

C.7.11.2 Meet Service Level Time To Respond (Acknowledge) to Requests Service Levels

After contacting support, the DOI requires an acknowledgement of the request and initial service center within the specified time to respond.

Table 15 Service Levels for Acknowledging Requests below identifies the tiers of service required by the DOI. Severity/Priority levels in Section C.7.10, Meet Customer and Program Support Service Levels.

Table 15 Service Levels for Acknowledging Requests

	Severity/Priority							
	1		2		3		4	
Service Band	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min	0 min	30 min	0 min	45 min	0 min	60 min
Band 2	15 min	2 hr	30 min	4 hr	45 min	6 hr	60 min	8 hr
Band 3	2 hr	8 hr	4 hr	16 hr	6 hr	24 hr	8 hr	36 hr
Band 4	8 hr	24 hr	16 hr	48 hr	24 hr	72 hr	36 hr	96 hr

C.7.11.3 Meet Mean-Time-To-Resolve Service Levels

The DOI requires a commitment on the mean time to resolve all service and support issues. Time is calculated from initial response until satisfactory resolution or escalation. Averages are calculated monthly.

Table 16 Service Levels for Mean-Time-To Resolve (Fix) below identifies the DOI required service bands, Severity/Priority levels in Section C.7.10, Meet Customer and Program Support Service Levels.

Table 16 Service Levels for Mean-Time-To Resolve

	Severity/Priority							
	1		2		3		4	
Service Band	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)	Minimum (>=)	Maximum (<)
Band 1	0 min	15 min	0 min	30 min	0 min	45 min	0 min	60 min
Band 2	15 min	2 hr	30 min	4 hr	45 min	6 hr	60 min	8 hr
Band 3	2 hr	8 hr	4 hr	16 hr	6 hr	24 hr	8 hr	36 hr
Band 4	8 hr	24 hr	16 hr	48 hr	24 hr	72 hr	36 hr	96 hr

C.7.11.4 Minimize Planned Downtime and Maintenance Windows

The Contractor shall provide support services that accommodate several maintenance window maximums. Planned downtime must occur at times specified in the individual task orders, and agreed upon with each application system owner. Proposed Service Bands for Scheduled Downtime are identified in Table 17 Scheduled Downtime Service Bands.

Table 17 Scheduled Downtime Service Bands

	Maximum Scheduled Downtime Per week	
Service Band	**Minimum (>=)**	**Maximum (<)**
Band 1 (High Availability)		**0.1 min**
Band 2	0.1 min	1 hr
Band 3	1 hr	2 hr
Band 4	2 hr	4 hr
Band 5	4 hr	8 hr

C.8 OPTIONAL CHARACTERISTICS REQUIREMENTS

Optional Characteristics Requirements define additional services that some systems require, but are not widespread enough to be considered a Resource or a Shared requirement.

C.8.1 Support Resource Segregation Options

The Contractor shall provide several options for segregating DOI resources:

- **a.** Fully segregated – DOI hosted systems (physical and virtual) must not share resources with any non-DOI entities. The Contractor shall provide physical barriers to separate customer's equipment.
- **b.** Federal government segregation – DOI hosted systems (physical and virtual) must not share resources with any non-Federal Government entities. The Contractor shall provide physical barriers to separate Federal government equipment from non-Federal government equipment.
- **c.** Non-segregated – DOI hosted systems (physical and virtual) can share resources with other entities.

Specific requirements for Resource Segregation may be identified in the individual Task Orders.

C.8.2 Support Non-production environments

The Contractor shall provide the ability to define non-production environments (e.g., test, development, training, staging, sandbox) as customized copies of a production environment. A non-production environment shall default to the same Resources, Service Level, and Feature requirements as the production environment, and a DOI administrator shall have the ability to adjust the non-production environment specifications.

Non-production environments may need access to Production storage or middleware instances, or may require separate clean storage and middleware instances. Non-production environments may require a means of populating storage from sources, both inside or outside, of the Contractor environment. The Contractor shall provide the ability to restrict access to non-production environments to a different set of users or "domains". For example, in relation to a Production environment a Development environment may have:

a. Same middleware and operating system Resource requirements
b. Lower Compute Host, Storage, and Bandwidth Resource requirements
c. Lower Service Level requirements
d. An option of Persistent or Non-persistent storage

The DOI shall have the ability to create and destroy non-production environments via web console.

Specific requirements Non-Production Environments may be identified in the individual Task Orders.

C.8.3 Support Requirement to Manage Underlying Physical Resources

The Contractor shall provide the functionality to manage the infrastructures underlying physical resources. For example, for licensing reasons, some systems need to attach a particular VM to a process and prevent it from being reassigned.

Specific requirements for Management of Underlying Physical Resources may be identified in the individual Task Orders.

C.8.4 Provide Content Delivery Network (CDN)

The Contractor shall provide the ability to cache static content at locations around the US to provide fast access to local users. This functionality is also known as Forward Staging.

Specific requirements for CDN may be identified in the individual Task Orders.

C.8.5 Support Government Compliance Requirements

The Contractor shall comply with government security and regulatory requirements that systems are subject to beyond those that the entire DOI is subject to. These regulations may include, but are not limited to:

- **a.** Ability to provide forensics on the roaming profiles of virtual desktop users
- **b.** Adherence to International Traffic in Arms Regulations (ITAR) requirements
- **c.** Adherence to Electronic Code of Federal Regulations (e-CFR) 250 regulations and Outer Continental Shelf (OCS) Lands Act
- **d.** Adherence to any restrictions placed on proprietary data stored by the Department
- **e.** Adherence to any litigation hold requirements currently in place or that may be imposed in the future
- **f.** Adherence to security controls defined in Section J, Attachment 1, DOI Security Control Standards

Government Compliance requirements may be identified in the individual Task Orders.

C.8.6 Support Alaska/Hawaii Regional Connectivity

The Contractor shall ensure users in Alaska and Hawaii can access core systems and data even when connectivity to CONUS has been lost. Definition of "core systems and data" must be configurable on a per application basis. Specific requirements for Regional Connectivity may be identified in the individual Task Orders.

C.8.7 Address Issues Related to Poor Connectivity

Please describe your approach for dealing with users in remote locations with poor, limited, or unstable internet connectivity (e.g., satellite, poor wireless coverage). Specific requirements for Poor Connectivity may be identified in the individual Task Orders.

C.8.8 Support or Provide Hardware Clustering

The Contractor shall provide capability to configure physical resources in a hardware cluster with a user configurable number of physical servers in the cluster. Specific requirements for Hardware Clustering may be identified in the individual Task Orders.

C.8.9 Provide Load Balancing

The Contractor shall provide the ability to distribute demand over multiple system instances. Specific requirements for Load Balancing may be identified in the individual Task Orders.

C.8.10 Support or Provide Interfaces to Non-Department Systems

The Contractor shall provide the ability to connect a Contractor hosted system or data store ("System A") to another system ("System B") that is hosted outside the DOI boundaries – example hosting locations include, but are not limited to:

a. Another government agency
b. A university
c. A private sector enterprise

The connection, up to and including the Contractor boundary, shall be configured to support data exchange with System B. This shall include, but is not limited to, any necessary DMZ, firewall, gateway configurations and maintenance.

The connection shall support authentication schemes required by either System A or System B. Included, but not limited to:

a. Active Directory
b. OpenID
c. Any other authentication schemes referred to in C.5.3 Establish and Maintain Security and Privacy

The connection shall adhere to all DOI security requirements including, but not limited to:

a. Encryption of all sensitive data in transit (motion) and at-rest (storage) using only NIST Validated FIPS 140-2 compliant and validated cryptographic modules and algorithms.

Specific requirements for Interfaces to Non-Departmental Systems may be identified in the individual Task Orders.

C.8.11 Support or Provide Static IP Addressing

The Contractor shall provide a static IP for a specified compute host instance. Specific requirements for Static IP Addressing may be identified in the individual Task Orders.

C.8.12 Provision Dedicated Resources

The Contractor shall provide the option to provision dedicated as well as shared units of the resources. Dedicated resources are defined as physical resources for which the provisioning system is the sole tenant. Specific requirements for Provisioning Dedicated Resources may be identified in the individual Task Orders.

C.9 ASSOCIATED SUPPORT SERVICES

Associated support services are those services which may be required to enable identification, analysis, prioritization, preparation and migration of IT systems from the current operating environment to the target operating environment, or may be required to ensure sustained operations and maintenance of systems in the target operating environment. Categories for

Associated Support Services are more completely described in Table 18 Associated Support Services.

Table 18 Associated Support Services

C.9.1	Planning Services--- includes cloud readiness evaluation for QASP & Pilot Transition Plan
C.9.2	Engineering Services
C.9.3	Migration Services---includes Management of Cloud Transition, Pilot Transition
C.9.4	Application Management Services
C.9.5	Interface Design and Integration Services
C.9.6	Testing- section 508 compliance
C.9.7	Training Services
C.9.8	Security Services

Specific requirements for Associated Support Services may be identified in the individual Task Orders.

SECTION D - PACKAGING AND MARKING

D.1 GENERAL

Any and all deliverables submitted under this contract shall be prepared and packaged in a cost-effective manner equivalent to standard commercial quality. Elaborate art work, expensive paper and bindings are neither necessary nor desired.

Unless otherwise directed by the Contracting Officer, all reports shall be delivered by electronic mail (e-mail) or First Class mail. The cost of delivery by more expensive means will be denied unless approval is obtained in advance from the Contracting Officer.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

SECTION E - INSPECTION AND ACCEPTANCE

E.1 52.252-2 - CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://farsite.hill.af.mil/vffar1.htm or https://www.acquisition.gov/far/, and DIAR Clauses: www.doi.gov/pam/aindex.html

Clause	Title	Date
52.203-3	Gratuities	Apr 1984
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	Oct 2010
52.204-4	Printed or Copied Double-Sided on Recycled Paper	May 2011
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.223-6	Drug-Free Workplace	May 2001
52.227-1	Authorization and Consent	Dec 2007
52.232-18	Availability of Funds	Apr 1984
52.242-13	Bankruptcy	July 1995
52.242-15	Stop-Work Order	Aug 1989

E.2 INSPECTION AND ACCEPTANCE

Inspection of the Supplies/Services provided hereunder shall be made by the Contracting Officer's Representative (COR) or any Inspectors designated by the Contracting Officer. The place of inspection for reports required under this contract shall be at the addresses for deliverables set forth in Section F. Final acceptance of Supplies/Services shall be made by the COR designated in the contract or as specified in individual orders.

E.2.1 General Acceptance Criteria

General quality measures, as set forth below, will be applied to each work product received from the contractor under this statement of work.

- Accuracy - Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity - Work Products shall be clear and concise. Any/All diagrams shall be easy to understand and be relevant to the supporting narrative.
- Consistency to Requirements - All work products must satisfy the requirements of this contract.
- File Editing - All text and diagrammatic files shall be editable by the Government.

- Format - Work Products shall be submitted in hard copy (where applicable) and in media mutually agreed upon prior to submission, unless otherwise specified herein. Hard copy formats shall follow any specified Directives or Manuals.

- Timeliness - Work Products shall be submitted on or before the due date specified herein or submitted in accordance with a later scheduled date determined by the Government.

E.3 QUALITY ASSURANCE

The COR or designated inspector will review, for completeness, preliminary or draft documentation that the Contractor submits, and may return it to the Contractor for correction. Absence of any comments by the COR will not relieve the Contractor of the responsibility for complying with the requirements of this work statement. Final approval and acceptance of documentation required herein shall be by letter of approval and acceptance by COR. The Contractor shall not construe any letter of acknowledgment of receipt material as a waiver of review, or as an acknowledgment that the material is in conformance with this work statement. Any approval given during preparation of the documentation, or approval for shipment shall not guarantee the final acceptance of the completed documentation.

SECTION F – DELIVERABLES OR PERFORMANCE

F.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://www.acquisition.gov/comp/far/loadmainre.html

CLAUSE	TITLE	DATE
52.247-34	**F.o.b. Destination**	**NOV 1991**

F.2 TERM OF THE CONTRACT

(a) The term of this contract will be three years from date of award, anticipated for May 1, 2013 through April 30, 2016. This is the base period of performance for this contract.

(b) This contract includes four (4) option periods, as shown below, for the renewal of the contract which may be unilaterally exercised by the Government. Each option period shall be exercised in accordance with Section I. See FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). All terms and conditions applicable to the base period shall apply to the options unless otherwise agreed upon.

- Option Period One (1) – May 1, 2016 through April 30, 2018
- Option Period Two (2) – May 1, 2018 through April 30, 2020
- Option Period Three (3) – May 1, 2020 through April 30, 2022
- Option Period Four (4) – May 1, 2022 through April 30, 2023

F.3 PLACE OF PERFORMANCE

Services may be provided off-site, on-site, or a combination of, depending on program requirements specified in individual task orders. However, the Government anticipates the majority of the work will be performed at the Contractor facilities unless otherwise stated in individual task orders.

F.4 MEETINGS, REPORTS AND OTHER DELIVERABLES

In fulfillment of this contract, the Contractor shall be required to provide deliverables. All deliverables shall be submitted to the Contracting Officer's Representative (COR), unless otherwise agreed upon.

Unless otherwise specified, the Government will have a maximum of ten (10) working days from the day the draft deliverable is received to review the document, provide comments back to the contractor, approve or disapprove the deliverable(s). The contractor will also have a maximum

of ten (10) working days from the day comments are received to incorporate all changes and submit the final deliverable to the Government. All days identified below are intended to be workdays unless otherwise specified.

F.4.1 Orientation Briefing

Within two (2) days from date of award, the contractor shall schedule an orientation briefing/initial strategy session. Both parties will mutually agree upon the specific date, time, and location of the briefing. The Government does not desire an elaborate orientation briefing nor does it expect the contractor to expend significant resources in preparation for this briefing. Rather, the intent of the briefing is to initiate the communication process between the Government and the contractor by introducing key participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of requirements and objectives, goals, constraints, policies, expected benefits, other relevant background information, and discussing near-term deliverables.

F.4.2 Deliverable Table

Unless otherwise agreed upon, all deliverables shall be submitted to the COR identified in Section G of this contract, with a copy of the transmittal letter to the Contracting Officer.

Reference	Milestone/Deliverable	Responsibility	Date
F.8	Subcontracting Plan Reports	Contractor	See F.8
C.5.2	Quarterly Contract and Service Line Service Management Conference Call	Contractor and Government	Quarterly
C.5.2.1.1	Role Based Report	Contractor	TBD at Orientation Briefing
C.5.2.1.3	Monitor Performance and Manage Alerts & Reporting Plan	Contractor	TBD at Orientation Briefing
C.5.2.1.4	Usage & Cost Monitoring Reports	Contractor	TBD at Orientation Briefing
C.5.2.1.5	Incident Management Report	Contractor	TBD at Orientation Briefing
C.5.2.4	Impact Plan	Contractor	TBD at Orientation Briefing
C.5.2.3	Quality Assurance Plan	Contractor	TBD at Orientation Briefing
C.5.3	Quarterly Security and Privacy Trends and Continual Improvement Meeting	Contractor and Government	Quarterly
C.5.3.3	Security Assessment Plan and Report	Contractor	TBD at Orientation Briefing
C.5.3.4	Mitigation Plan	Contractor	TBD at Orientation Briefing
C.6	Annual Technology and Architecture Review	Contractor and Government	Annual
C.7	Quarterly Service Level Review	Contractor and Government	Quarterly
C.7.4	Disaster Recovery Plan	Contractor	TBD at Orientation Briefing
F.4.1	Orientation Briefing Schedule	Contractor	TBD
F.6.1	Transition-Out Plan	Contractor	no later than ninety (90) calendar days prior to the expiration of the contract period, unless another date is mutually agreed upon

F.5 OTHER PERFORMANCE REQUIREMENTS

F.5.1 Productive Direct Labor Hours

The contractor can only charge the Government for "Productive Direct Labor Hours". "Productive Direct Labor Hours" are defined as those hours expended by Contractor personnel in performing work under this effort. This does not include sick leave, vacation, Government or contractor holidays, jury duty, military leave, or any other kind of administrative leave such as acts of God (i.e., hurricanes, snow storms, tornadoes, etc.), Presidential funerals or any other unexpected government closures.

F.5.2 Legal Holidays

The following Government holidays are normally observed by Government personnel: New Years Day, Martin Luther King's Birthday, Presidential Inauguration Day (metropolitan DC area only), President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, Christmas Day, and any other day designated by Federal Statute, Executive Order, and/or Presidential Proclamation. Or any other kind of administrative leave such as acts of God (i.e., hurricanes, snow storms, tornadoes, etc.), Presidential funerals or any other unexpected government closures. When a holiday falls on Saturday or Sunday, it is observed on the adjacent Friday or Monday, respectively.

F.6 TRANSITION PLANS

F.6.1. Transition Out -- At the end of the period of performance, the incumbent contractor shall transition activities to the incoming contractor with minimal disruption of services to the government. The contractor shall maintain sufficient qualified staff to meet all requirements of this effort services. The contractor shall submit a written phase-out plan to the COR no later than ninety (90) calendar days prior to the expiration of the contract period, unless otherwise agreed upon. The plan shall detail phase-out activities to assure continuity of operations and the execution of a smooth and timely transition. Phase-out activities shall be coordinated through the COR. The outgoing contractor shall submit a weekly status report of phase-out activities to the COR beginning the 7th calendar day following the award of a successor contract until otherwise notified by the COR to discontinue.

F.7 NOTICE TO THE GOVERNMENT OF DELAYS

(a) In the event the Contractor encounters difficulty in meeting performance requirements, or when it anticipates difficulty in complying with the contract delivery schedule or any date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the Contracting Officer and the Contracting Officer's Representative, in writing, giving pertinent details, provided that this data shall be informational only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or date or of any rights or remedies provided by law or under this contract.

(b) If the Contractor fails to respond in a timely manner to any portion of this contract, delay will be attributed to the Contractor. Although the period of performance may change due to the delay, the price may be subject to a downward adjustment.

(c) If the Government delays performance of this contract, the period of performance and/or price may be revised upon mutual agreement between the Government and the Contractor.

F.8 SUBCONTRACTING PLAN REPORTS

(a) The Contractor shall submit a report for subcontracting under this particular contract and/or a summary report on subcontracts in all contracts between the Contractor and the Department of the Interior which contain subcontract goals for awards to small business, small disadvantaged business concerns, HUB zone business, service-disabled veteran owned small businesses, or woman-owned business. Reports will be prepared and submitted electronically in accordance with the instructions at the electronic Subcontract Reporting System (eSRS) accessible at www.esrs.gov.

(b) Individual Contract Report data (formerly Standard Form 294) is due on the 25th day following the close of the reporting period, unless the contract incorporates the contractor's approved, annual company-wide or division-wide commercial product plan. Summary Report data (formerly Standard Form 295) is due 30 days after the close of the Government's fiscal year. Paper copies of these reports are no longer required.

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 AUTHORITIES

Notwithstanding the Contractor's responsibility for total management during the performance of this contract, administration of the contract will require maximum coordination between the Government and the Contractor. The following information identifies the individuals responsible for this coordination.

G.1.1 Authority – Contracting Officer (CO)/Administrator, Contracting Officer's Representative (COR) and Contractor's Project Manager

G.1.1.1 Contracting Officer (CO) and/or Contract Specialist (CS) - The CO/CS for this contract is:

Name: Terrie L. Callahan, Contracting Officer
Department of the Interior, NBC, AQD
381 Elden Street, 4th Floor
Herndon, VA 20170
Phone/Fax: 703-964-3596
Email: Terrie_Callahan@nbc.gov

Name: Rob Stoltz, Contract Specialist
Department of the Interior, NBC, AQD
381 Elden Street, 4th Floor
Phone/Fax: 703-964-3624
Email: Rob_Stoltz@nbc.gov

A Contracting Officer, in accordance with Subpart 1.6 of the Federal Acquisition Regulation, is the only person authorized to make or approve any changes in any of the requirements of this contract, and notwithstanding any clauses contained elsewhere in this contract, the said authority remains solely with a Contracting Officer. In the event the Contractor makes any changes at the direction of any person other than a Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in cost incurred as a result thereof.

G.1.1.2 Contracting Officer's Representative (COR)

Name: Peggy FinneFrock
Department of the Interior, Office of the Chief Information Officer (OCIO)
PO Box 25487
Lakewood, CO 80225-0487
Phone: 303-236-5090
Email: Peggy-lee_Finnefrock@ios.doi.gov

All contractual questions and concerns will be directed to the Government Contracting Officer. The Government Contracting Officer is the only individual with the authority to financially obligate the government and to make changes to original terms and conditions of this task order .

The contractor is responsible for notifying the contracting officer of any potential issues or concerns – technical, scope or financial, concerning this task order.

The Contracting Officer (CO) is the exclusive agent of the Government with authority to enter into and administer contracts. The CO must therefore ensure that all requirements of law and regulation are followed. As the CO's representative, the COR is authorized to act in the stead of the CO to monitor the technical effort being performed under this task order. The COR must become very familiar with the requirements of this task order and communicate with the Contractor to ensure the Contractor is making satisfactory progress in performance of this task order. Other than the CO, the COR is the only Government employee who may direct the flow of matters between the Government and the Contractor. Additionally, the COR is limited to directing the flow of *technical* matters, and no other matters.

A contract is a legally enforceable agreement that sets forth the rights and responsibilities of the parties thereto. If the Contractor deviates from the terms of this task order, it is a matter between the Government (represented by the CO) and the Contractor. The COR must therefore keep the CO fully informed so that effective solutions can be applied to problems as soon as they develop. The COR will be required to exercise his/her best judgment to determine what matters deserve the attention of the CO. When in doubt, report the matter to the CO.

COR suggestions to the Contractor about what must be done to fulfill the terms of this task order may lead to unauthorized commitments by the Government for additional compensation or to a release of the Contractor from its obligations under this task order. The COR must therefore refrain from communicating with the Contractor about matters that are outside the flow of *technical matters*. If in doubt, ask the CO. While the COR can and must make technical decisions, the COR may not take any contractual administration actions unless they are clearly authorized by a COR appointment.

1. An appointed COR is authorized and required to:

a. Inspect and monitor the Contractor's performance to assure technical compliance with this task order. Immediately notify the CO of non-compliance, failure to make due progress, or a dispute. The COR should refer all discussions concerning disputed matters to the CO.

b. For all contracts for the National Business Center (NBC), input data on all Contractor employees into NBC's Electronic Staffing (eCStaffing) database https://ecstaff.nbc.gov. Ensure that the data is accurate and is updated and maintained as necessary throughout the life of this task order.

c. Inspect and verify satisfactory delivery of all services and products, including the Contractor's reports.

d. Verify efficient and satisfactory performance of work for payment purposes. When contracts contain a warranty or maintenance clause, immediately notify the CO and the Contractor of any deficiencies. After you have completed the notification, monitor the Contractor's response. Notify the CO if the Contractor fails to comply with the requirements in a timely fashion.

e. For the Herndon offices, within five business days of receiving an invoice or an electronic notification through IPP (www.ipp.gov) enter on the first page of a paper invoice, or in the appropriate space in IPP for an electronic invoice, the recommended action whether to Approve, Reject or Partially Approve the invoice. The COR *must* make invoice action recommendations on Debit Invoices and/or Credit Vouchers/Memos before IPP can forward them for CO approval. Submit paper invoices to invoices@aqd.nbc.gov – or the designated individual who forwarded the invoice for signature; you *must sign and date the invoice.*

f. For offices other than Herndon, the COR must take action within five business days of receiving a paper invoice. The COR *must* record the recommended action whether to Approve, Reject or Partially Approve the invoice, and must sign and date the invoice. Follow the invoicing instructions set forth herein for forwarding the invoice after COR approval or rejection.

2. When exercising COR duties under this appointment, the COR is responsible for:

a. Knowing and understanding the terms and conditions of this task order. Immediately discuss any unclear areas with the CO;

b. Knowing the scope and limitations of the COR authority and using good judgment, skill, and reasonable care in exercising it;

c. Protecting privileged and sensitive procurement information;

d. Monitoring the work site periodically to verify progress and informing the CO of the findings concerning:

(1) Actual performance vs. scheduled performance.
(2) Action needed to restore this effort to schedule;

e. Implementing the Government Furnished Property/Materials (GFP/M) contract provisions, when applicable. COR responsibilities for GFP/M include: providing the CO with any proposed changes, additions, or deletions to GFP/M; ensuring that delivery is made on time; and inspecting each unit upon its return and notifying the CO of any deficiencies;

f. Monitoring the results of all required tests within the stated time limitations. The results must be promptly forwarded to the CO. When equipment is delivered to more than one site, ensuring the CO is informed in writing (e.g., e-mail) of delivery and acceptance. Ensuring that equipment is not installed or repaired by Government personnel when the responsibility lies with the Contractor;

g. Documenting actions taken and decisions that have made as the COR, and maintain adequate records to describe sufficiently the performance of the duties as COR during the life of this task order. As a minimum, the COR file should contain copies of the following:
(1) COR appointment memorandum
(2) Task Order award and any modifications
(3) All correspondence
(4) Records of COR inspections
(5) Records of conversations with the contractor
(6) Invoices and vouchers;

h. Providing the CO with a copy of any correspondence (including e-mail) you send to the Contractor;

i. Assuring that the Contractor has access to the facility as well as appropriate clearances for personnel to have access to classified or sensitive material, when applicable, as soon as it is determined that access to such material will be required;

j. Reviewing and recommending to the CO approval/disapproval of Contractor's requests for public release of information regarding work being performed under this task order;

k. Maintaining current COR certification throughout the appointment. In accordance with Office of Management and Budget memorandum dated September 6, 2011, Subject: The Federal Acquisition Certification for Contracting Officer Technical Representatives, CORs must have a minimum of 40 hours of training and must maintain their skills currency through continuous learning. Twenty-two of the required 40 hours of training hours must cover the essential COR competencies. The remaining 18 hours of the required 40 hours of training should include agency-specific courses, electives, and/or those identified by the COR's supervisor, in consultation with the Contracting Officer, as necessary, for managing a particular contract. To maintain a FAC-COR, CORs are required to earn 40 continuous learning points (CLPs) of skills currency training every two years.

l. Immediately notifying the CO of an impending COR change in order to facilitate a smooth transition and early training of the new COR; and

m. Monitoring the performance and dollars expended on time-and-material and labor- hour type line items or contracts to ensure that they appear to be reasonable for the efforts performed; this includes the type of labor and number of labor

hours, travel (including locations, duration, and number of travelers), and types and quantities of material.

The COR shall only authorize or approve contractually funded travel expenses which comply with Federal Travel Regulations or Joint Travel Regulation, as appropriate. As a minimum, the COR must review invoices and any status reports provided by the Contractor to verify that the hours and costs incurred are reasonable in view of the Contractor's effort and deliverables provided. The COR must also review invoices to ensure that the labor rates charged are the same as those set forth in this task order.

This task order is covered by the Prompt Payment Act which subjects the Government to penalties if invoices are not paid in a timely fashion. Penalties are assessed if payment is not made within 30 days after receipt of a proper invoice or final acceptance of the goods or services, whichever is later.

To avoid paying late payment penalties from your program funds, it is important that the COR promptly accept/reject delivered goods or services and immediately certify invoices for payment. Payment, inspection, and acceptance procedures are set forth in this task order. Notify the CO immediately if goods or services are rejected. Ensure invoices include proper justification for rejected or partially paid invoices.

The COR must ensure that Contractor employees and consultants with access to Government information technology systems complete the required background investigation forms. The COR must ensure these forms are submitted to the Agency security officer or personnel security specialist for screening and processing. Prior to granting access to Government IT applications and systems the COR must verify that Contractor employees and consultants meet the mandatory training requirements of OMB Circular A-130 and 5 CFR Part 930.

The COR may face personal pecuniary liability if you commit unauthorized acts that obligate the Government to pay for work that is outside the scope of this task order. It is therefore essential for the COR to understand that under the COR appointment, the COR must *NOT*:

a. Modify the stated terms and conditions of this task order or the scope of work in any manner. All such changes must be made in writing by the CO;
b. Award, execute, or agree to any contract, contract modification, accord, task or delivery order, notice of intent, or any similar agreement;
c. Obligate the Government, in any way, to make any payment of money outside the terms and conditions of this task order;
d. Make a final decision on any contractual matter that is subject to the Disputes Clause at FAR 52.233-1;
e. Terminate the Contractor's right to proceed, or impose or place a demand upon the Contractor to perform any task or permit any substitution not specifically provided for in this task order;
f. Change the period of performance;
g. Authorize purchases not provided for under this task order;
h. Authorize the use of overtime;

i. Furnish or authorize the furnishing of Government property, except as required under this task order;
j. Direct the activities of any employee of the Contractor, except as specifically provided for under this task order;
k. Authorize subcontracting or the use of consultants not already authorized under this task order;
l. Grant deviations from or waive any of the terms or conditions of this task order; or
m. Make any change that affects price, quality, quantity, delivery, or other terms and conditions of this task order.

The COR may *not* delegate any of the duties or responsibilities assigned to you under this appointment, and should ensure that an Alternate COR is appointed to perform duties in the event of your absence.

An appointment as COR will end on the earliest of the following events:
1. Task Order completion.
2. Task Order termination.
3. Leaving present duty position.
4. The CO's termination of this appointment.

When performing COR duties under a COR appointment, the COR shall maintain an arms-length relationship with the Contractor and consistently strive to protect the interests of the Government. The COR should be particularly attentive to possible violations of the False Claims Amendments Act of 1986 and the Program Fraud Civil Remedies Act of 1986, which involve the submission of false claims or the making of false statements. Similarly, the COR shall avoid any act that may tend to compromise the integrity or apparent integrity of yourself or the Government, or which interferes with the Contractor's right to perform.

Gratuities offered to the COR or any other Government official by any private person or company must be reported to the CO. In the capacity as the COR, the COR is responsible for promptly notifying the CO of any suspected violations of the Gratuities Clause, FAR 52.203-3.

If the COR has or intends to obtain any direct or indirect financial interest which conflicts with your duty to promote and protect the interests of the United States (this includes any discussion of employment with the Contractor), the COR shall immediately advise his/her supervisor and the CO of the conflict. The COR shall also avoid the appearance of any such conflict to maintain public confidence in the Government's conduct of business with the private sector.

For additional information on COR duties and responsibilities please refer to the Federal Acquisition Institute's online COR Training Modules at www.fai.gov.

G.1.1.3 Supervision of Contractor's Employees

The Contractor shall be responsible for managing and overseeing the activities of all Contractor personnel, as well as subcontractor efforts used in performance of this effort. The Contractor's management responsibilities shall include all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained herein. Resumes submitted for employees assigned to perform under this contract shall contain documented experience directly applicable to the functions to be performed. Further, these prior work experiences shall be specific and of sufficient variety and duration that the employee is able to effectively and efficiently perform the functions assigned.

If the Contractor finds clarification necessary with respect to the scope of services to be performed or the manner in which the services are to be performed hereunder, he shall request in writing such clarification from the Contracting Officer.

Contractor personnel shall not at any time during the contract period be employees of the U.S. Government.

The contractor's employees and subcontractors must make clear, in dealings with the public, federal employees, or other contractors that they are not federal employees. To minimize possible confusion, contractors and subcontractors are not permitted to wear clothing or other items (apart from official identity credential) bearing the name, logo, or seal of the U.S. Department of the Interior while performing work under this contract.

G.1.1.3.1 Contractor's Representative

The Contractor shall provide a Project Manager to facilitate Government-Contractor communications. The Project Manager shall be the primary technical and managerial interface between the Contractor and Contracting Officer (CO) and the Contracting Officer's Technical Representative (COR) located at the DOI Facility identified below. The name of this person, and an alternate or alternates, who shall act for the contractor when the Manager is absent, be designated in writing to the CO. The Project Manager or alternate will have full authority to act for the contractor on all contract matters relating to daily operations. The Contractor's designated Project manager for this contract is:

Name: ***TBD at Orientation Briefing***
Address:
Phone:
Fax:
Email:

The Contractor's designated Project manager for this contract shall have the authority to make any no-cost contract technical, hiring and dismissal decision, or special arrangements regarding this contract.

The Project manager shall have full authority to act for the Contractor in the performance of the required services. The Project manager or a designated representative shall meet

with the CO/COR as necessary to maintain satisfactory performance and to resolve any issues pertaining to Government/Contractor procedures. At these meetings, a mutual effort will be made to resolve any and all problems identified. Written minutes of these meetings shall be prepared by the Contractor, signed by the Contractor's designated representative, and furnished to the Government within two (2) workdays of the subject meeting. The Project manager, and all designated representatives, shall be able to fluently read, write, and speak the English language.

The Project Manager or alternate must be available during normal duty hours, as specified herein and to meet with government personnel within 24 hours notification to discuss problems.

The Project Manager may not be diverted to other projects for 14 consecutive days or more without giving prior written notification to the contracting officer or his representative. Such notification shall include a justification for the diversion, together with information on the proposed substitute in sufficient detail to permit analysis of any potential negative effects on contract performance. No substitution shall be made without the written consent of the contracting officer; provided, however, that the contracting officer may grant such consent retroactively. Any such substitution of a permanent nature will be made a part of this contract through the issuance of a modification.

When the Project Manager is temporarily unavailable to manage the contract effort for a period longer than 72 hours, including absences due to vacation or illness, the contractor will provide to the COR a written designation of an alternate representative, itemizing any limitations in the alternate's authority. The procedures of paragraph (b) above do not apply to such temporary designations unless they are expected to exceed the time period indicated in that paragraph.

G.2 OTHER ADMINISTRATIVE CONSIDERATIONS

G.2.1 Correspondence

To promote timely and effective administration, correspondence shall be subject to the following procedures:

(a) Technical correspondence (where technical issues relating to compliance with the requirements herein) shall be addressed to the Contracting Officer's Representative (COR) with an information copy to the Contracting Officer (CO).

(b) All other correspondence, including invoices, (that which proposes or otherwise involves waivers, deviations or modifications to the requirements, terms or conditions of this SOW) shall be addressed to the Contracting Officer with an information copy to the COR.

G.2.2 Electronic Invoicing and Payment Requirements – Invoice Processing Platform (IPP) (September 2011)

Payment requests must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP).

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions – Commercial Items included in commercial item contracts. The IPP website address is: https://www.ipp.gov. The Contractor must use the IPP website to register, access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in CCR) will receive enrollment instructions via email from the Federal Reserve Bank of Boston (FRBB) within 3 – 5 business days of the contract award date. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email ippgroup@bos.frb.org or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the contracting officer with its proposal or quotation.

G.2.2.1 Additional Invoicing Instructions

Any payment under this task order to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. The Contractor shall bill either monthly or quarterly, in arrears, in accordance with 31 U.S.C 3324.

G.3 METHOD OF PAYMENT

The Department of the Interior has adopted the Department of Defense's Central Contractor Registration database as its database for contractor information. All payments by the Government under this contract shall be made by electronic funds transfer (EFT). Therefore, the provisions of FAR 52-232.33, Payment by Electronic Funds Transfer – Central Contractor Registration, apply and are hereby incorporated by reference in Section I of this contract.

G.4 PAYMENT FOR UNAUTHORIZED WORK

No payments will be made for any unauthorized supplies and/or services, or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor of their own volition or at the request of an individual other than a duly appointed Contracting Officer. Only a duly appointed Contracting Officer is authorized to change the specifications, terms, and conditions under this effort.

G.5 DIAPR 2010-18 AUTHORITIES AND DELEGATIONS (INTERIM - MAY 2010)

(a) The Contracting Officer is the only individual authorized to enter into or terminate this contract, modify any term or condition of this contract, waive any requirement of this contract, or accept nonconforming work.

(b) The Contracting Officer will designate a Contracting Officer's Representative (COR) at time of award. The COR will be responsible for technical monitoring of the contractor's performance and deliveries. The COR will be appointed in writing, and a copy of the appointment will be furnished to the Contractor. Changes to this delegation will be made by written changes to the existing appointment or by issuance of a new appointment. The contractor will be notified of the name and other contact information of the COR/COTR, once they are established.

(c) The COR is not authorized to perform, formally or informally, any of the following actions:

(1) Promise, award, agree to award, or execute any contract, contract modification, or notice of intent that changes or may change this contract;
(2) Waive or agree to modification of the delivery schedule;
(3) Make any final decision on any contract matter subject to the Disputes Clause;
(4) Terminate, for any reason, the Contractor's right to proceed;
(5) Obligate in any way, the payment of money by the Government.

(d) The Contractor shall comply with the written or oral direction of the Contracting Officer or authorized representative(s) acting within the scope and authority of the appointment memorandum. The Contractor need not proceed with direction that it considers to have been issued without proper authority. The Contractor shall notify the Contracting Officer in writing, with as much detail as possible, when the COR has taken an action or has issued direction (written or oral) that the Contractor considers to exceed the COR's appointment, within 3 days of the occurrence. Unless otherwise provided in this contract, the Contractor assumes all costs, risks, liabilities, and consequences of performing any work it is directed to perform that falls within any of the categories defined in paragraph (c) prior to receipt of the Contracting Officer's response issued under paragraph (e) of this clause.

(e) The Contracting Officer shall respond in writing within 30 days to any notice made under paragraph (d) of this clause. A failure of the parties to agree upon the nature of a direction, or upon the contract action to be taken with respect thereto , shall be subject to the provisions of the Disputes clause of this contract.

(f) The Contractor shall provide copies of all correspondence to the Contracting Officer and the COR.

(g) Any action(s) taken by the Contractor, in response to any direction given by any person acting on behalf of the Government or any Government official other than the Contracting Officer or the COR acting within his or her appointment, shall be at the Contractor's risk. (End of notice)

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 ADVERTISING OF AWARD

The contractor shall not refer to this award in commercial advertising, or similar promotions in such a manner as to state or to imply that the product or services provided is endorsed, preferred, or is considered superior to other products or services by the Department of the Interior (DOI). This includes advertising, or similar promotions, in all forms or electronic, broadcast, and print media.

In addition, the contractor is restricted from reproducing the image(s) of the DOI in any form of commercial advertising, or similar promotion. This includes images of official seals and buildings. The reproduction of official seals and the images of buildings is a matter controlled by regulation and Executive Order. Any proposed usage of such symbols must be brought to the attention of the Contracting Officer.

H.2 PRINTING

The Contractor shall not engage in, nor subcontract for, any printing (as that term is defined in Title I of the Government Printing and Binding Regulations in effect on the effective date of this contract) in connection with the performance of work under this contract provided, however, that performance of a requirement under this contract involving the reproduction of less than 5,000 production units of any one page, or less than 25,000 production units in the aggregate of multiple pages, will not be deemed to be printing. A production unit is defined as one sheet, size 8.5 x 11 inches, one side only one color.

H.3 KEY PERSONNEL

Any key personnel applicable to this acquisition shall be identified in the individual task orders.

H.4 CONTRACTOR INTERFACES

The Contractor and/or his subcontractors may be required as part of the performance of this contract to work with other Contractors supporting the IT Transformation Initiative for the Government. Such other Contractors shall not direct this Contractor and/or their subcontractors in any manner. Also, this Contractor and/or their subcontractors shall not direct the work of other Contractors in any manner.

The Government shall establish an initial contact between the Contractor and other Contractors and shall participate in an initial meeting at which the conventions for the scheduling and conduct of future meetings/contacts will be established. Any CORs of other efforts shall be included in any establishment of conventions.

H.5 WARRANTY AGAINST DUAL COMPENSATION

The contractor warrants that if he/she is involved in two or more projects, at least one of which is supported by Federal funds, he/she may not be compensated for more than 100% of his/her time during any part of the period of dual involvement.

H.6 RESTRICTIONS ON FUTURE CONTRACTING WITH DOI

It is agreed by the parties to this contract that the contractor will be restricted in its future contracting with DOI in the manner described herein. Except as specifically stated herein, the contractor shall compete for DOI business on an equal basis with other companies.

If the contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work which are to be incorporated into a solicitation, the contractor will be ineligible to perform the work described within that solicitation as a prime or first-tier subcontractor under the resultant contract. Such restrictions shall remain in effect for three (3) years following completion of work under this contract. DOI will not unilaterally require the contractor to prepare such specifications or statements of work under this contract.

The restrictions as stated herein may be waived by the Contracting Officer if it is determined that such restrictions would be detrimental to any Government program.

H.7 RESERVED

H.8 DISPOSITION OF MATERIAL

Upon termination or completion of all work under this contract, the Contractor shall prepare for shipment, deliver f.o.b. destination, or dispose of all materials received from the Government and all residual materials produced in connection with the performance of this contract as may be directed by the Contracting Officer, or as specified in other provisions of this contract. All materials produced or required to be delivered under this contract become and remain the property of the Government.

H.9 CONFIDENTIALITY OF DATA

a) The work under this contract requires access to proprietary, business confidential, or financial data of other companies and/or Government internal scientific, planning or procurement sensitive/source selection data, which, if released to third parties may give unfair business, technical, or competitive advantages. As long as such data remains proprietary or business confidential, the contractor shall protect such data from unauthorized use and disclosure and agrees not to use it to compete with such companies or for any purpose other than performance of this contract.

b) This data may be in various forms, such as documents, raw photographic films, magnetic or digital media, photographic prints, computer system data, or it may be interpretative results derived from analysis, investigative, or study effort. Regardless of the form of this data, the contractor agrees that neither it nor any of its employees will disclose to third parties any such data, or derivatives thereof, except as may be required in the performance of this contract. Further, the contractor will not copy any of this data, or derivatives thereof, other than as necessary for the performance of this contract.

c) The contractor will establish policies and procedures to implement the substance of this clause at the individual employee level which will assure that affected employees are made aware of the contract provision and the contractor's implementing policies and procedures. Particular attention will be given to keeping employees advised of statutes and regulations applicable to the handling of third party confidential or financial data.

d) This clause does not preclude the contractor and/or its employees from independently acquiring and using data from legitimate sources outside of this contract, or from performing and using independent analysis of data so acquired, provided that the contractor and/or its employees fully document the source of such data, and the independence of any such analysis.

e) The Contractor shall immediately notify, in writing, the Contracting Officer in the event that the Contractor determines or has reason to suspect a breach of this requirement.

f) The contractor will insert the substance of this clause in each subcontract hereunder (other than for purchase of supplies or equipment) unless the Contracting Officer has waived this requirement, in writing, as to particular subcontracts or classes of subcontracts.

g) Any unauthorized disclosure of information may result in termination of this contract for cause.

H.10 SECTION 508 APPLICABLE STANDARDS

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), individuals with disabilities must have access to and use of information and data that is comparable to individuals without disabilities. Requirements for accessibility based on Section 508 are determined to be relevant for cloud computing. The following requirements apply to this acquisition.

- 36 CFR Section 1194.21 – Software Applications and Operating Systems
- 36 CFR Section 1194.22 – Web-based Internet Information and Applications
- 36 CFR Section 1194.23 – Telecommunication Products
- 36 CFR Section 1194.24 – Video and Multimedia Products
- 36 CFR Section 1194.31 – Functional Performance Criteria
- 36 CFR Section 1194.41 – Information, Documentation, and Support

A description of the Section 508 standards is located at http://www.section508.gov/index.cfm?fuseAction=stdsdoc.

H.11 TITLE TO MATERIALS

Other than the rights and interests expressly set forth in this agreement, the Government retains exclusive right, title, and interest (including but not limited to intellectual property rights and licenses) in and to all its data. Government data includes, without limitation, the results of any processing of Government data that occurs on any Contractor provided system. The Contractor acquires no rights or licenses through this agreement (including but not limited to intellectual property rights or licenses) to use the Government's data for its own purposes. The Contractor does not acquire and may not claim any security interest in the data.

The Government retains the right to access and retrieve its data stored on the Contractor's service infrastructure at its sole discretion and in an accessible (i.e., nonproprietary) format.

H.12 INDEMNITY

The Contractor shall hold and save the Government, its officers, agents and employees, harmless from liability of any nature or kind, including costs and expenses to which they may be subject, for or on account of any or all suits or damages of any character whatsoever resulting from injuries or damages sustained by any person or persons or property by virtue of performance of this contract, arising or resulting in whole or in part from the fault, negligence, wrongful act or wrong mission of the Contractor, or any subcontractor, or their employees, agents, etc.

Nothing in paragraph a above shall be considered to preclude the Government from receiving the benefits of any insurance the Contractor may carry which provides for the indemnification of any loss or destruction of, or damages to property in the custody and care of the Contractor where such lass, destruction or damage is the Government property. The Contractor shall do nothing to prejudice the Government's right to recover against third parties for any loss, destruction of, or damage to Government property, and upon the request of the Contracting Officer shall, at the Government's expense, furnish the Government all reasonable assistance and cooperation (including assistance in the prosecution of suit and the execution of instruments of assignment in favor of the Government) in obtaining recovery.

The contractor agrees to include this clause, appropriately modified, in all subcontracts to be performed under this contract.

H.13 AUTHORITY TO OBLIGATE THE GOVERNMENT

The Contracting Officer is the only individual who can legally commit or obligate the Government to the expenditure of public funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract and/or task order or specific authorization from the Contracting Officer.

H.14 TECHNOLOGY REFRESH/ENHANCEMENT (TRE) PROPOSALS

During the performance of this contract, the Government may solicit, and at the Contractor's discretion may submit Technology Refresh/Enhancement (TRE) Proposals. TRE means any changes and/or enhancements within the service areas and/or service lines contained in this contract. This may include any service areas and/or service lines that are not specified within the contract as long as they are within the general scope. The TRE shall contain the documentation by which any proposed change is described, justified, and submitted to the procuring activity for approval or disapproval. These TREs, must be within the general scope of this contract, may be requested by the Government and/or proposed by the contractor, for certain requirements specified herein. The TREs may include but are not limited to enhancements, technology refresh or renewal, and/or for any other purpose which present a system or service performance advantage to the Government. Improvement in technology which better provides for the needs of employees/users with disabilities is especially encouraged. Implementation of an approved TRE may occur by either a supplemental agreement or, if appropriate, as a written change order to the contract. Additionally, the DOI considers Data Center Consolidation or emergency operations requirements, and any hosting and associated support services necessary, to be within scope of this contract. Therefore, any modifications and/or task orders maybe be executed for any requirements within this area. This would include Contractor operation and maintenance of Government owned assets within either Government or Contractor owned and operated facilities.

a) At a minimum, any proposal submitted by the Contractor pursuant to this clause shall include the following information:
   1) A statement to the effect that the proposal is being submitted pursuant to this clause;
   2) A detailed technical description of the proposed changes;
   3) A detailed comparison between the existing contract requirements and the proposed changes, including the advantages and disadvantages of each;
   4) An itemized list of each contract requirement, including any delivery schedules or completion dates that would, in the Contractor's opinion, be effected by the proposed changes;
   5) An estimate of any change (increase or decrease) to the contract's price, including any related cost;
   6) An estimate of the date by which the Government should accept the proposal in order to receive maximum benefits; and,
   7) The date until which the proposal is valid. (This date must provide reasonable time for the Government to review the proposal.)

b) The Contractor may withdraw, in whole or in part, any improvement proposal which is not accepted by the Government within the specified time for acceptance.

c) The Contracting Officer shall accept or reject any improvement proposal by giving the Contractor written notice of such acceptance or rejection.

d) If the proposal is accepted, the Contracting Officer shall issue a contract modification to incorporate any necessary changes into the contract, including any increase or decrease in the contract price. Such adjustment shall be made in accordance with the changes clause of this contract.

e) Unless and until the contract is modified in writing to incorporate any changes resulting from the Government's acceptance of an improvement proposal, the Contractor shall continue to perform in accordance with the contract's existing terms and conditions.

f) The Contracting Officer's decision to accept or reject any improvement proposal shall be final and shall not be subject to the terms cited in the disputes clause. Furthermore, the Government shall not be liable for the direct reimbursement of any proposal costs. In no event shall the Government be liable for any additional costs incurred by the Contractor due to the Government's delay in accepting or rejecting any improvement proposal.

g) The Contractor is requested to identify specifically any information contained in its improvement proposal which it considers confidential and/or proprietary and which it prefers not be disclosed outside the Government. The Contractor's identification of information as confidential and/or proprietary is for informational purposes only and shall not be binding on the Government. The Contractor is advised that such information may be subject to releases under the Freedom of Information Act (5 U.S.C. 552).

H.15 OFF RAMP

a) To ensure success of the Foundation Cloud Hosting Services, each Contractor is expected to participate in the ordering process by submitting proposals in response to task order requests (TORs) for which the Contractor has a reasonable chance for award, to successfully perform the terms of their Orders, and to promptly improve performance when it does not meet the terms of the Orders. If a Contractor does not meet these expectations, it is the Government's intent to "off-ramp" the Contractor by:

b) Permitting such Contract to expire instead of exercising the Option; or

c) Implementing a termination for convenience (if applicable and only if such action is in the Government's best interest); or

d) Implementing a termination for default, if applicable; or

e) Taking any other action which may be permitted under the Foundation Cloud Hosting Services Contract's terms and conditions.

H.16 ON RAMP

Consistent with FAR 16.504(c)(1)(ii)(A), the Contracting Officer has determined it is in the Government's best interest that at all times during the term of the Contract, there remain an adequate number of Contractors eligible to compete for Orders. Over time, the total number of Contractors may fluctuate due to various reasons including industry consolidation, significant changes in the marketplace or advances in technology, general economic conditions, the Government's exercise of the off-ramp process, or other reasons. Recognizing this, DOI intends to periodically review the total number of Contractors participating in the Foundation Cloud Hosting Services Ordering Process and determine whether it would be in the Government's best interest to initiate an open season to add new contractors to the Basic Contract.

H.17 OPEN SEASON PROCEDURES

If DOI determines that it would be in the Government's best interest to open a new solicitation to add new contractors to this contract, the Contracting Officer may do so at any time provided:

a) The solicitation is issued under then-applicable federal procurement law;

b) The solicitation identifies the total approximate number of new awards that the Contracting Officer intends to make. The Contracting Officer may decide to award more or fewer Contracts than the number anticipated in the solicitation depending upon the overall quality of the offers received and also reserves the right to limit open season to only small business concerns;

c) Any Contractor that meets the eligibility requirements set forth in the new solicitation submits a proposal in response to the solicitation; however, existing Contractors may not hold more than one contract at any time;

d) The award decision under any solicitation is based upon substantially the same evaluation factors/sub-factors as the original solicitation;

e) The terms and conditions of any resulting awards from a new solicitation are materially identical to the existing version of the Contract;

f) The term for any such new awards from a solicitation is co-terminus with the existing term for all other Contractors, including the option period (if applicable); and

g) If awarded a contract, any new Contractor is eligible to submit a proposal in response to any task order requests and receive task order awards with the same rights and obligations as any other Contractor.

H.18 GOVERNMENT OPERATIONAL READINESS ASSESSMENT TESTING (GORAT)

H.18.1 Pre-Award GORAT

The Government, at its discretion, may require pre-award testing, upon identification of the apparent awardee, for any subsequently issued task orders. Task order award maybe contingent upon successful completion of capability and performance demonstrations and pre-award testing, which may include, but is not limited to demonstration in the following objective areas: Performance, usability, flexibility and extensibility of the solution. However, the scope and time frame of the pre-award GORAT will be as specified in the task order.

H.18.2 POST-Award GORAT

Upon award of a task order issued under this IDIQ contract, the Government reserves the right to conduct a post-award GORAT and will be specified within the individual task order(s). The Government and Contractor will cooperate to complete initial GORAT Testing. The scope and time frame of the post-award GORAT will be as specified in the task order.

H.19 FAIR OPPORTUNITY ORDERING

H.19.1 General

Individual orders will describe services to be performed or supplies to be delivered so that the full price for the performance of the work can be established when the order is placed. Orders will be within the scope of the contract, will be issued within the period of performance, will be within the maximum value of the contract, and will follow the fair opportunity process as described below. However, the Government reserves the right to set aside individual task orders under this contract for small businesses, or to include an evaluation preference for small businesses on individual task orders, provided there is a reasonable expectation of receiving responses from sufficient small business sources to ensure adequate competition in terms of fair and reasonable price, technical quality, and/or delivery. In accordance with FAR 16.505(b)(6), to ensure all contractors are afforded a fair opportunity to be considered for award, consistent with procedures in the contract the Competition Advocate is designated as OMBUDSMAN.

Orders may be issued any time during the term of the contract or any extension. All orders issued before the end of the contract term shall be honored and performed by the contractor, following the terms and conditions of the contract. All orders are subject to the terms and conditions of this contract. In the event of a conflict between an order and this contract, the contract shall prevail.

H.19.2 Fair Opportunity Process

The following fair opportunity process will be utilized in placing orders against this contact in order to provide all contractors, within their technical service lines(s), a fair opportunity to be considered for an order.

The fair opportunity process described in the Federal Acquisition Regulation (FAR) 16.505(b) and the Draft Order Guide, see Section J, Attachment 45, applies to this contract. The Government will provide a fair opportunity to all awardees within the applicable Service Model, except as provided for in paragraph H.19.3, Exceptions to Fair Opportunity, of this section.

The Government reserves the right to modify this process, including the Draft Ordering Guide, and will notify the contractor of any such modifications in advance of any orders being placed using the modified process without additional cost to the Government. Additionally, the Government reserves the right to issue orders orally, by facsimile, or by any other electronic commerce methods.

H.19.3 Exceptions to Fair Opportunity

Orders may be issued without the fair opportunity process whenever circumstances warrant the exercise of any exception set forth in 41 United States Code (USC) §253j.

Certain Agencies may have additional requirements for use of an exception to the fair opportunity process. Under those circumstances, the Agency or an Agency conducting the fair opportunity process on behalf of another Agency must meet the Agency's additional requirements. Agencies will consider the following in conducting and documenting the fair opportunity order placement decision. These examples are provided only for illustrative purposes:

The following describes the possible exceptions and examples that an Agency may determine apply under this contract.

- Exception Provided for by 41 USC §253j
- Examples that Qualify as Exceptions
  - Unusual urgency that would lead to unacceptable delays
  - Natural disaster or other emergency
  - Military/mobilization
  - Immediate short-term need arising on short notice
  - Only one capable contractor
  - Only one contractor offers service
  - Only one contractor offers service to locations needed
  - Only one contractor can demonstrate it is capable of providing service as required by user or to required locations
  - Economy, efficiency, and logical follow-on to an order already issued under Fair Consideration
  - Orders placed to minimize inefficiencies or additional costs that would result from introducing multiple maintenance, operations, training, or other support systems
  - Need to satisfy Minimum Guarantees

H.19.4 Protests and Complaints

No protest under FAR Subpart 33.1 is authorized in connection with the issuance or proposed issuance of an order under this contract, except for a protest on the grounds that the order increases the scope, period, or maximum value of the contract (10 U.S.C. 2304c(e) and 41 U.S.C. 253j(d)) and in accordance with FAR Subpart 16.505.

H.20 EARNED VALUE MANAGEMENT SYSTEM (July 2006)

(a) The Contractor shall use an earned value management system (EVMS) that has been determined by the Cognizant Federal Agency (CFA) to be compliant with the guidelines in ANSI/EIA Standard - 748 (current version at the time of award) to manage this contract. If the Contractor's current EVMS has not been determined compliant at the time of award, see paragraph (b) of this clause. The Contractor shall submit reports in accordance with the requirements of this contract.

(b) If, at the time of award, the Contractor's EVM System has not been determined by the CFA as complying with EVMS guidelines or the Contractor does not have an existing cost/schedule control system that is compliant with the guidelines in ANSI/EIA Standard - 748 (current version at time of award), the Contractor shall—
(1) Apply the current system to the contract; and
(2) Take necessary actions to meet the milestones in the Contractor's EVMS plan approved by the Contracting Officer.

(c) The Government will conduct an Integrated Baseline Review (IBR). If a pre-award IBR has not been conducted, a post award IBR shall be conducted as early as practicable after contract award.
(1) Exercise of significant options; or
(2) Incorporation of major modifications.

(d) The Contracting Officer may require an IBR at—

(e) Unless a waiver is granted by the CFA, Contractor proposed EVMS changes require approval of the CFA prior to implementation. The CFA will advise the Contractor of the acceptability of such changes within 30 calendar days after receipt of the notice of proposed changes from the Contractor. If the advance approval requirements are waived by the CFA, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(f) The Contractor shall provide access to all pertinent records and data requested by the Contracting Officer or a duly authorized representative as necessary to permit Government surveillance to ensure that the EVMS conforms, and continues to conform, with the performance criteria referenced in paragraph (a) of this clause.

(g) The Contractor shall require the subcontractors specified below to comply with the requirements of this clause:

All subcontractors as identified in the Contractor's proposal dated November 19, 2012, submitted in response to the Foundation Cloud Hosting Solicitation, D12PS00316, are hereby required to comply with the terms and conditions of this clause, unless otherwise agreed upon. This also applies to any subsequent task orders.

(End of clause)

H.21 CONTRACTOR'S PROPOSAL

The contractor's proposal dated November 19, 2012, is hereby incorporated into this contract by reference with the same force and effect as if included in full text. Any conflict between and terms and conditions of this contract and the contractor's proposal, shall be resolved by giving precedence to the terms and conditions contain in this contract.

SECTION I - CONTRACT CLAUSES

I.1 FAR 52.252-2 – CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): FAR Clauses: http://www.acquisition.gov/comp/far/loadmainre.html and DIAR Clauses: http://farsite.hill.af.mil/vfdiara.htm

Clause	Title	Date
52.202-1	Definitions	JAN 2012
52.203-3	Gratuities	APR 1984
52.203-5	Convenant Against Contingent Fees	APR 1984
52.203-6	Restrictions on Subcontractor Sales to the Government	SEPT 2006
52.203-7	Anti-Kickback Procedures	OCT 2010
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	JAN 1997
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	OCT 2010
52.204-4	Printed or Copied Double-Sided on Recycled Paper	MAY 2011
52.204-7	Central Contractor Registration	FEB 2012
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	DEC 2010
52.215-8	Order of Precedence--Uniform Contract Format	OCT 1997
52.215-11	Price Reduction for Defective Cost or Pricing Data—Modifications	AUG 2011
52.215-17	Waiver of Facilities Capital Cost of Money	OCT 1997
52.215-21	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data—Modifications	OCT 2010
52.216-2	Economic Price Adjustment – Standard Supplies	JAN 1997
52.216-4	Economic Price Adjustment – Labor and Materials	JAN 1997
52.216-5	Price Redetermination – Prospective	OCT 1997
52.216-7	Allowable Cost and Payment	JUN 2011
52.217-2	Cancellation Under Multi-year Contracts	OCT 1997
52.219-4	Notice of Price Evaluation preference for HUBZone Small Business Concerns	JAN 2011
52.219-8	Utilization of Small Business Concerns	JAN 2011
52.219-9	Small Business Subcontracting Plan ALT II – OCT 2001	JAN 2011
52.219-16	Liquidated Damages—Subcontracting Plan	JAN 1999
52.219-24	Small Disadvantaged Business Participation Program—Targets	OCT 2000

Clause	Title	Date
52.219-28	Post Award Small Business Program Representation	APR 2012
52.222-2	Payment for Overtime Premiums	JUL 1990
52.222-3	Convict Labor	JUN 2003
52.222-4	Contract Work Hours and Safety Standards Act—Overtime Compensation	JUL 2005
52.222-21	Prohibition of Segregated Facilities	FEB 1999
52.222-26	Equal Opportunity	MAR 2007
52.222-29	Notification of Visa Denial	JUN 2003
52.222-35	Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans	SEPT 2010
52.222-36	Affirmative Action for Workers with Disabilities	OCT 2010
52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans	SEP 2010
52.222-38	Compliance with Veterans' Employment Reporting Requirements	SEP 2010
52.222-41	Service Contract Act of 1965	NOV 2007
52.222-43	Fair Labor Standards Act and Service Contract Act – Price Adjustment (Multiple Year and Option Contracts)	SEP 2009
52.223-5	Pollution Prevention and Right-to-Know Information	MAY 2011
52.223-6	Drug-Free Workplace	MAY 2001
52.223-10	Waste Reduction Program	MAY 2011
52.223-15	Energy Efficiency in Energy-Consuming Products	DEC 2007
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	AUG 2011
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.225-25	Prohibition on Contracting with Entities Engaging in Sanctioned Activities Relating to Iran—Representation and Certification	NOV 2011
52.227-1	Authorization and Consent	DEC 2007
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	DEC 2007
52.227-3	Patent Indemnity	APR 1984
52.227-14	Rights in Data—General ALT II – DEC 2007 ALT III – DEC 2007	DEC 2007
52.227-16	Additional Data Rights Requirements	JUN 1987
52.227-17	Rights in Data—Special Works	DEC 2007
52.227-18	Rights in Data—Exiting Works	DEC 2007
52.228-5	Insurance—Work on a Government Installation	JAN 1997
52.228-7	Insurance—Liability to Third Persons	MAR 1996
52.229-3	Federal, State, and Local Taxes	APR 2003
52.232-1	Payments	APR 1984

Clause	Title	Date
52.232-7	Payments under Time-and-Materials and Labor-Hour Contracts	FEB 2007
52.232-8	Discount for Prompt Payment	FEB 2002
52.232-9	Limitation on Withholding of Payments	APR 1984
52.232-17	Interest	OCT 2010
52.232-18	Availability of Funds	APR 1984
52.232-19	Availability of Funds for the Next Fiscal Year Fill-in: TBD at Task Order Award	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-23	Assignment of Claims	JAN 1986
52.232-25	Prompt Payment	OCT 2008
52.232-33	Payment by Electronic Funds Transfer--Central Contractor Registration	OCT 2003
52.233-1	Disputes--Alternate I	DEC 1991
52.233-3	Protest After Award	AUG 1996
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.234-3	Notice of Earned Value Management System - Post Award IBR	JUL 2006
52.234-4	Earned Value Management System.	JUL 2006
52.237-2	Protection of Government Buildings, Equipment and Vegetation	APR 1984
52.237-3	Continuity of Services	JAN 1991
52.237-10	Identification of Uncompensated Overtime	OCT 1997
52.242-13	Bankruptcy	JUL 1995
52.243-1	Changes—Fixed Price	AUG 1987
52.243-3	Changes—Time-and-Materials or Labor-Hours	SEPT 2000
52.244-2	Subcontracts Fill-in: (d) TBD at Task Order Awards (j) TBD at Task Order Awards	OCT 2010
52.244-5	Competition in Subcontracting	DEC 1996
52.245-1	Government Property	APR 2012
52.246-25	Limitation of Liability—Services	FEB 1997
52.247-1	Commercial Bill of Lading Notations	FEB 2006
52.247-63	Preference for U.S. – Flag Air Carriers	JUN 2003
52.247-64	Preference for Privately Owned U.S. – Flag Commercial Vessels	FEB 2006
52.248-1	Value Engineering	OCT 2010
52.249-2	Termination for Convenience of the Government (Fixed Price)	APR 2012
52.249-8	Default (Fixed-Price Supply and Service)	APR 1984
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012
52.251-2	Interagency Fleet Management System Vehicles and Related Services	JAN 1991
52.253-1	Computer Generated Forms	JAN 1991
1452.224-1	Privacy Act Notification (Deviation)	JUL 1996

I.2 Department of the Interior Acquisition Regulation (DIAR)

The contract clauses set forth in the following paragraphs of the Department of the Interior Acquisition Regulation (DIAR) are incorporated in this contract with the same force and effect as though set forth herein in full text. The designated clauses are incorporated as they appear in the DIAR on the date of this contract, notwithstanding the date referenced.

Clause	Title	Date
1452.215-70	Examination of Records by the DOI	APR 1984
1452.228-70	Liability Insurance—DOI	JULY 1996

I.3 FAR 52.203-10 – PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY (Jan 1997)

(a) The Government, at its election, may reduce the price of a fixed-price type contract and the total cost and fee under a cost-type contract by the amount of profit or fee determined as set forth in paragraph (b) of this clause if the head of the contracting activity or designee determines that there was a violation of subsection 27(a), (b), or (c) of the Office of Federal Procurement Policy Act, as amended (41 U.S.C. 423), as implemented in section 3.104 of the Federal Acquisition Regulation.

(b) The price or fee reduction referred to in paragraph (a) of this clause shall be—

(1) For cost-plus-fixed-fee contracts, the amount of the fee specified in the contract at the time of award;

(2) For cost-plus-incentive-fee contracts, the target fee specified in the contract at the time of award, notwithstanding any minimum fee or "fee floor" specified in the contract;

(3) For cost-plus-award-fee contracts—

(i) The base fee established in the contract at the time of contract award;

(ii) If no base fee is specified in the contract, 30 percent of the amount of each award fee otherwise payable to the Contractor for each award fee evaluation period or at each award fee determination point.

(4) For fixed-price-incentive contracts, the Government may—

(i) Reduce the contract target price and contract target profit both by an amount equal to the initial target profit specified in the contract at the time of contract award; or

(ii) If an immediate adjustment to the contract target price and contract target profit would have a significant adverse impact on the incentive price revision relationship under the contract, or adversely affect the contract financing provisions, the Contracting Officer may defer such adjustment until establishment of the total final price of the contract. The total final price established in accordance with the incentive price revision provisions of the contract shall be reduced by an amount equal to the initial target profit specified in the contract at the time of contract award and such reduced price shall be the total final contract price.

(5) For firm-fixed-price contracts, by 10 percent of the initial contract price or a profit amount determined by the Contracting Officer from records or documents in existence prior to the date of the contract award.

(c) The Government may, at its election, reduce a prime contractor's price or fee in accordance with the procedures of paragraph (b) of this clause for violations of the Act by its subcontractors by an amount not to exceed the amount of profit or fee reflected in the subcontract at the time the subcontract was first definitively priced.

(d) In addition to the remedies in paragraphs (a) and (c) of this clause, the Government may terminate this contract for default. The rights and remedies of the Government specified herein are not exclusive, and are in addition to any other rights and remedies provided by law or under this contract.

(End of clause)

I.4 FAR 52.216-24 LIMITATION OF GOVERNMENT LIABILITY (APR 1984)

(a) In performing this contract, the Contractor is not authorized to make expenditures or incur obligations exceeding current obligated dollars.

(b) The maximum amount for which the Government shall be liable if this contract is terminated is the negotiated settlement dollars.

(End of clause)

I.5 FAR 52.217-8 – OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within any time prior to expiration of the current period of performance.

(End of clause)

I.6 FAR 52.217-9 – OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within any time prior to the end of the current contract period; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty (30) calendar days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed ten (10) years.

(End of clause)

I.7 FAR 52.216-18 ORDERING (Oct 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from date of award through the end of any current option or base period of this contract.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of clause)

I.8 FAR 52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) *Minimum order*. When the Government requires supplies or services covered by this contract in an amount of less than $5,000, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order*. The Contractor is not obligated to honor—

1) Any order for a single item in excess of $1,000,000,000;
2) Any order for a combination of items in excess of $1,000,000,000; or
3) A series of orders from the same ordering office within one (1) day(s) that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (*i.e.*, includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within two (2) days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

I.9 FAR 52.216-22 INDEFINITE QUANTITY (Oct 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; *provided,* that the Contractor shall not be required to make any deliveries under this contract after the expiration date of the current period of performance or individual order, whichever is later.

(End of clause)

I.10 FAR 52.252-6 – AUTHORIZED DEVIATION IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Department of the Interior Acquisition Regulation (48 CFR Chapter 14) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

I.11 DEPARTMENT OF THE INTERIOR ACQUISITION REGULATION (DIAR)

The contract clauses set forth as follows are the Department of the Interior Acquisition Regulation (DIAR) clause.

I.11.1 1452.203-70, Restriction on Endorsements—DOI (JUL 1996)

The Contractor shall not refer to contracts awarded by the Department of the Interior in commercial advertising, as defined in FAR 31.205-1, in a manner which states or implies that the product or service provided is approved or endorsed by the Government, or is considered by the Government to be superior to other products or services. This restriction is intended to avoid the appearance of preference by the Government toward any product or service. The Contractor may request the Contracting Officer to make a determination as to the propriety of promotional material.

(End of clause)

I.11.2 1452.204-70, Release of Claims—DOI (JUL 1996)

After completion of work and prior to final payment, the Contractor shall furnish the Contracting Officer with a release of claims against the United States relating to this contract. The Release of Claims form (DI-137) shall be used for this purpose. The form provides for exception of specified claims from operation of the release.

(End of clause)

I.11.3 1452.215-71, Use and Disclosure of Proposal Information (APR 1984)

(a) Definitions. For the purposes of this provision and the Freedom of Information Act (5 U.S.C. 552), the following terms shall have the meaning set forth below:
(1) "Trade Secret" means an unpatented, secret, commercially valuable plan, appliance, formula, or process, which is used for making, preparing, compounding, treating or processing articles or materials which are trade commodities.
(2) "Confidential commercial or financial information" means any business information (other than trade secrets) which is exempt from the mandatory disclosure requirement of the Freedom of Information Act, 5 U.S.C. 552. Exemptions from mandatory disclosure which may be applicable to business information contained in proposals include exemption (4), which covers "commercial and financial information obtained from a person and privileged or confidential," and exemption (9), which covers "geological and geophysical information, including maps, concerning wells."

(b) If the offeror, or its subcontractor(s), believes that the proposal contains trade secrets or confidential commercial or financial information exempt from disclosure under the Freedom of Information Act, (5 U.S.C. 552), the cover page of each copy of the proposal shall be marked with the following legend:

"The information specifically identified on pages _____ of this proposal constitutes trade secrets or confidential commercial and financial information which the offeror believes to be exempt from disclosure under the Freedom of Information Act. The offeror requests that this information not be disclosed to the public, except as may be required by law. The offeror also requests that this information not be used in whole or part by the government for any purpose other than to evaluate the proposal, except that if a contract is awarded to the offeror as a result of or in connection with the submission of the proposal, the Government shall have the right to use the information to the extent provided in the contract."

(c) The offeror shall also specifically identify trade secret information and confidential commercial and financial information on the pages of the proposal on which it appears and shall mark each such page with the following legend:

"This page contains trade secrets or confidential commercial and financial information which the offeror believes to be exempt from disclosure under the Freedom of Information Act and which is subject to the legend contained on the cover page of this proposal."

(d) Information in a proposal identified by an offeror as trade secret information or confidential commercial and financial information shall be used by the Government only for the purpose of evaluating the proposal, except that (i) if a contract is awarded to the offeror as a result of or in connection with submission of the proposal, the Government shall have the right to use the information as provided in the contract, and (ii) if the same information is obtained from another source without restriction it may be used without restriction.

(e) If a request under the Freedom of Information Act seeks access to information in a proposal identified as trade secret information or confidential commercial and financial information, full consideration will be given to the offeror's view that the information constitutes trade secrets or confidential commercial or financial information. The offeror will also be promptly notified of

the request and given an opportunity to provide additional evidence and argument in support of its position, unless administratively unfeasible to do so. If it is determined that information claimed by the offeror to be trade secret information or confidential commercial or financial information is not exempt from disclosure under the Freedom of Information Act, the offeror will be notified of this determination prior to disclosure of the information.

(f) The Government assumes no liability for the disclosure or use of information contained in a proposal if not marked in accordance with paragraphs (b) and (c) of this provision. If a request under the Freedom of Information Act is made for information in a proposal not marked in accordance with paragraphs (b) and (c) of this provision, the offeror concerned shall be promptly notified of the request and given an opportunity to provide its position to the Government. However, failure of an offeror to mark information contained in a proposal as trade secret information or confidential commercial or financial information will be treated by the Government as evidence that the information is not exempt from disclosure under the Freedom of Information Act, absent a showing that the failure to mark was due to unusual or extenuating circumstances, such as a showing that the offeror had intended to mark, but that markings were omitted from the offeror's proposal due to clerical error.

(End of provision)

SECTION J – LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

Table of Contents

Attachment #	Title	# of Pages
Attachment 1	*DOI Security Control Standards*	
	• Security Assessment and Authorization	11
	• Access Control	21
	• Audit and Accountability	12
	• Awareness and Training	7
	• Configuration Management	14
	• Contingency Planning	12
	• Identification and Authentication	12
	• Incident Response	10
	• Maintenance	10
	• Media Protection	11
	• Personnel Security	9
	• Physical and Environmental Protection	15
	• Planning	8
	• Program Management	10
	• Risk Assessment	9
	• System and Communication Protection	21
	• System and Information Integrity	13
	• System and Service Acquisition	14
Attachment 2	*Foundation Cloud Hosting Services (FCHS) Information Technology Security and Privacy Requirements for the DOI*	35
Attachment 3	*DOI Privacy Loss Plan*	
	• Departmental Privacy Loss Mitigation Strategy	1
	• DOI Privacy Loss Mitigation Strategy (PLMS)	43
	• Identity Theft Task Force Charter	8
Attachment 4	*Additional Information Technology Information*	
	• Departmental Manual, Part 375-IRM Program Management	8
	• Role Based Security Training (RBST) Standard	19
	• Electronic Mail Gateway Security Reference Architecture	41
	• Domain Name System (DNS) Security Reference Architecture	28
	• Plan of Action and Milestones (POA&M) Process Standard	118
Attachment 5	*Foundation Cloud Hosting Services DRAFT Ordering Guide*	3

Department of the Interior

Security Control Standard

System and Service Acquisition

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 28, 2011	Initial draft
Timothy Brown	0.2	January 31, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: SYSTEM AND SERVICES AQUISITION 5

SA-1 SYSTEM AND SERVICES ACQUISTION POLICY AND PROCEDURES 5
SA-2 ALLOCATION OF RESOURCES 6
SA-3 LIFE CYCLE SUPPORT 6
SA-4 AQUISITIONS 7
SA-5 INFORMATION SYSTEM DOCUMENTATION 8
SA-6 SOFTWARE USAGE RESTRICTIONS 9
SA-7 USER INSTALLED SOFTWARE 9
SA-8 SECURITY ENGINEERING PRINCIPLES 10
SA-9 EXTERNAL INFORMATION SYSTEM SERVICES 10
SA-10 DEVELOPER CONFIGURATION MANAGEMENT 11
SA-11 DEVELOPER SECURITY TESTING 12
SA-12 SUPPLY CHAIN PROTECTION 13
SA-13 TRUSTWORTHINESS 13

SECURITY CONTROL STANDARD: SYSTEM AND SERVICES AQUISITION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 System and Services Acquisition (SA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

SA-1 SYSTEM AND SERVICES ACQUISTION POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM- 9.

Control Enhancements: None.
References: NIST Special Publications 800-12, 800-100

Priority and Baseline Allocation:

P1	**LOW** SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Applicability: All Information Systems

Control: The organization:

a. Includes a determination of information security requirements for the information system in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Related controls: PM-3, PM-11.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Priority and Baseline Allocation:

P1	**LOW** SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Applicability: All Information Systems

Control: The organization:

a. Manages the information system using a system development life cycle methodology that includes information security considerations ;
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.

Supplemental Guidance: Related control: PM-7.

Control Enhancements: None.

References: NIST Special Publication 800-64.

Priority and Baseline Allocation:

P1	**LOW** SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 AQUISITIONS

Applicability: All Information Systems

Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

a. Security functional requirements/specifications;
b. Security-related documentation requirements; and
c. Developmental and evaluation-related assurance requirements.

Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements for federal information systems.
Control Enhancements:

1. The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.
2. The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.
4. The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

7. The organization:

   a. Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and
   b. Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.

References: ISO/IEC 15408; FIPS 140-2; NIST Special Publications 800-23, 800-35, 800-36, 800-64, 800-70; Web: WWW.NIAP-CCEVS.ORG.

Priority and Baseline Allocation:

P1	**LOW** SA-4	**MOD** SA-4 (1) (4) (7)	**HIGH** SA-4 (1) (2) (4) (7)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Applicability: All Information Systems

Control: The organization:

a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
   - Secure configuration, installation, and operation of the information system;
   - Effective use and maintenance of security features/functions; and
   - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged)
   - functions; and

b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
   - User-accessible security features/functions and how to effectively use those security features/functions;
   - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
   - User responsibilities in maintaining the security of the information and information system; and

c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

Control Enhancements:

1. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.
2. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.
3. The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SA-5	**MOD** SA-5 (1) (3)	**HIGH** SA-5 (1) (2) (3)

SA-6 SOFTWARE USAGE RESTRICTIONS

Applicability: All Information Systems

Control: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SA-6	**MOD** SA-6	**HIGH** SA-6

SA-7 USER INSTALLED SOFTWARE

Applicability: All Information Systems

Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW SA-7	MOD SA-7	HIGH SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Applicability: Moderate and High Impact Information Systems

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SA-8	HIGH SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Applicability: All Information Systems

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Control Enhancements:

1. The organization:

    a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
    b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined senior organizational official*].

Enhancement Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	LOW SA-9	MOD SA-9 (1)	HIGH SA-9 (1)

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Applicability: Moderate and High Impact Information Systems

Control: The organization requires that information system developers/integrators:

a. Perform configuration management during information system design, development, implementation, and operation;
b. Manage and control changes to the information system;
c. Implement only organization-approved changes;
d. Document approved changes to the information system; and
e. Track security flaws and flaw resolution.

Supplemental Guidance: Related controls: CM-3, CM-4, CM-9.

Control Enhancements: None Mandated.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-10	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING

Applicability: Moderate and High Impact Information Systems

Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

a. Create and implement a security test and evaluation plan;
b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
c. Document the results of the security testing/evaluation and flaw remediation processes.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.

Control Enhancements:

1. The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SA-11 (1)	**HIGH** SA-11(1)

SA-12 SUPPLY CHAIN PROTECTION

Applicability: Moderate and High Impact Information Systems

Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

d. Create and implement a security test and evaluation plan;
e. implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
f. Document the results of the security testing/evaluation and flaw remediation processes.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	MOD SA-12	**HIGH** SA-12

SA-13 TRUSTWORTHINESS

Applicability: High Impact Information Systems

Control: The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].

Supplemental Guidance: The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include: (i) *security functionality* (i.e., the security features or functions employed within the system); and (ii) *security assurance* (i.e., the grounds for confidence that the security functionality is effective in its application).

Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained

by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Minimum assurance requirements are described in Appendix E.

Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyber attacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of information technology components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results. Related controls: RA-2, SA-4, SA-8, SC-3.

Control Enhancements: None Mandated.

References: FIPS Publications 199, 200; NIST Special Publications 800-53, 800-53A, 800-60, 800-64.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-13

Department of the Interior

Security Control Standard

Access Control

July 2011

Version: 1.3

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	November 30, 2010	Initial draft
Timothy Brown	0.2	December 02, 2010	Incorporated comments into body text
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Added cloud controls to "high"
Chris Peterson	1.0	February 17, 2011	Final review of controls; remove margin notes
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	May 5, 2011	Incorporated language under AC-20 addressing use of GFE vs non-GFE
Lawrence K. Ruffin	1.3	July 26, 2011	Modified language in AC-20 to eliminate specific reference to WPA2(AES) and instead refer to applicable NIST standards; and modified AC-8 to incorporate the DOI approved content for system use notification messages or banners

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: ACCESS CONTROL **5**

AC-1 ACCESS CONTROL POLICY AND PROCEDURES 5
AC-2 ACCOUNT MANAGEMENT 6
AC-3 ACCESS ENFORCEMENT 7
AC-4 INFORMATION FLOW ENFORCEMENT 8
AC-5 SEPARATION OF DUTIES 9
AC-6 LEAST PRIVILEGE 9
AC-7 UNSUCCESSFUL LOGIN ATTEMPTS 10
AC-8 SYSTEM USE NOTIFICATION 11
AC-10 CONCURRENT SESSION CONTROL 12
AC-11 SESSION LOCK 13
AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION/AUTHENTICATION 13
AC-16 SECURITY ATTRIBUTES 14
AC-17 REMOTE ACCESS 14
AC-18 WIRELESS ACCESS 16
AC-19 ACCESS CONTROL FOR MOBILE DEVICES 17
AC-20 USE OF EXTERNAL INFORMATION SYSTEMS 18
AC-22 PUBLICLY ACCESSIBLE CONTENT 21

SECURITY CONTROL STANDARD: ACCESS CONTROL

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Access Control (AC) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

a) A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b) Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1

AC-2 ACCOUNT MANAGEMENT

Applicability: All Information Systems

Control: The organization manages information system accounts, including:

a) Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
b) Establishing conditions for group membership;
c) Identifying authorized users of the information system and specifying access privileges;
d) Requiring appropriate approvals for requests to establish accounts;
e) Establishing, activating, modifying, disabling, and removing accounts;
f) Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
g) Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
h) Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
i) Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
j) Reviewing accounts annually.

Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

1. The organization employs automated mechanisms to support the management of information system accounts.
2. The information system automatically terminates temporary and emergency accounts after 90 days.
3. The information system automatically disables inactive accounts after 90 days.
4. The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

7. The organization:
    1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and
    2. Tracks and monitors privileged role assignments.

    Enhancement Supplemental Guidance: Privileged roles include, but are not limited to: key management, network and system administration, database administration, web administration.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-2	**MOD** AC-2 (1) (2) (3) (4) (7)	**HIGH** AC-2 (1) (2) (3) (4) (7)

AC-3 ACCESS ENFORCEMENT

Applicability: All Information Systems

Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

3. The information system enforces role-based access control over all users and resources where the policy rule set for each policy specifies:
    a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and
    b. Required relationships among the access control information to permit access.

    Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, Mandatory Access Control, and Originator Controlled Access Control. Nondiscretionary access control policies may be employed by organizations in addition to the employment of discretionary access control policies.

For Mandatory Access Control (MAC): Policy establishes coverage over all subjects and objects under its control to ensure that each user receives only that information to which the user is authorized access based on classification of the information, and on user clearance and formal access authorization. The information system assigns appropriate security attributes (e.g., labels/security domains/types) to subjects and objects, and uses these attributes as the basis for MAC decisions. The Bell-LaPadula security model defines allowed access with regard to an organization-defined set of strictly hierarchical security levels as follows: A subject can read an object only if the security level of the subject dominates the security level of the object and a subject can write to an object only if two conditions are met: the security level of the object dominates the security level of the subject, and the security level of the user's clearance dominates the security level of the object (no read up, no write down).

For Role-Based Access Control (RBAC): Policy establishes coverage over all users and resources to ensure that access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role.

References: None.

Priority and Baseline Allocation:

P1	LOW AC-3	MOD AC-3 (3)	HIGH AC-3 (3)

AC-4 INFORMATION FLOW ENFORCEMENT

Applicability: Moderate and High Impact Information Systems

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-4	HIGH AC-4

AC-5 SEPARATION OF DUTIES

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related controls: AC-3.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

AC-6 LEAST PRIVILEGE

Applicability: Moderate and High Impact Information Systems

Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.

Control Enhancements:

1. The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*].

   Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.

2. The organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

   Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of *role* is intended to address those situations where an access control policy such as *Role Based Access Control (RBAC)* is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2)	HIGH AC-6 (1) (2)

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Applicability: All Information Systems

Control: The information system:

a. Enforces a limit of no more than three consecutive invalid login attempts, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles (e.g., the USGCB and FDCC allow for no more than five consecutive invalid login attempts, and the enhancement supplemental guidance for the DOI Identification and Authentication IA-5 Authenticator Management control standard allows for mobile devices to be configured for ten failed login attempts under specified conditions after which they must be automatically wiped), by a user during a 15 minute period; and
b. Automatically locks the account/node for 30 minutes when the maximum number of unsuccessful attempts is exceeded, unless specified and allowed to be less by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles (e.g., the USGCB and FDCC allow for automatic unlock after 15 minutes). The control applies regardless of whether the login occurs via a local or network connection.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period

established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

Control Enhancements: None.

References: NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB); Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.

Priority and Baseline Allocation:

P1	**LOW** AC-7	**MOD** AC-7	**HIGH** AC-7

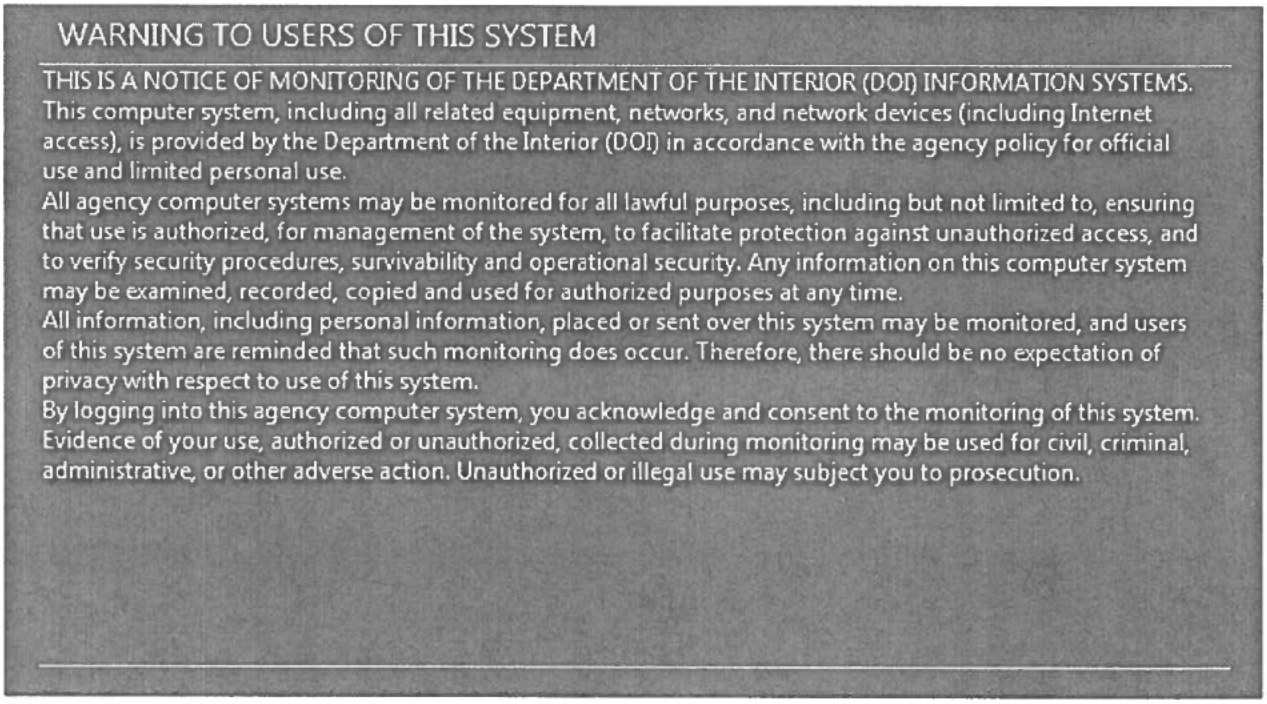
AC-8 SYSTEM USE NOTIFICATION

Applicability: All Information Systems

Control: The information system:

a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;
b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist. The DOI approved content for system use notification messages or banners is provided below.



Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-8	**MOD** AC-8	**HIGH** AC-8

AC-10 CONCURRENT SESSION CONTROL

Applicability: Moderate and High Impact Information Systems

Control: The information system limits the number of concurrent sessions for each system account to 1 session.

Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD AC-10**	**HIGH** AC-10

AC-11 SESSION LOCK

Applicability: Moderate and High Impact Information Systems

Control: The information system:

a. Prevents further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

1. The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB); Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** AC-11 (1)	**HIGH** AC-11 (1)

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION/AUTHENTICATION

Applicability: All Information Systems

Control: The organization:

a. Identifies specific user actions that can be performed on the information system without identification or authentication; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

Supplemental Guidance: This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such

instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred. Related control: CP-2, IA-2.

Control Enhancements:

1. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

References: None.

Priority and Baseline Allocation:

P1	LOW AC-14	MOD AC-14 (1)	HIGH AC-14 (1)

AC-16 SECURITY ATTRIBUTES

Applicability: Moderate and High Impact Information Systems

Control: The information system supports and maintains the binding of [*Assignment: organization defined security attributes*] to information in storage, in process, and in transmission.

Control Enhancements: None mandated.

Priority and Baseline Allocation:

P0	LOW Not Selected	MOD AC-16	HIGH AC-16

AC-17 REMOTE ACCESS

Applicability: All Information Systems

Control: The organization:

a. Documents allowed methods of remote access to the information system;
b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
c. Monitors for unauthorized remote access to the information system;
d. Authorizes remote access to the information system prior to connection; and
e. Enforces requirements for remote connections to the information system.

Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the

organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.

Control Enhancements:

1. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

   Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

2. The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

   Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.

3. The information system routes all remote accesses through a limited number of managed access control points.

   Enhancement Supplemental Guidance: Related control: SC-7.

4. The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

   Enhancement Supplemental Guidance: Related control: AC-6.

5. The organization monitors for unauthorized remote connections to the information system continuously in real time, and takes appropriate action if an unauthorized connection is discovered.

7. The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization defined additional security measures*] and are audited.

   Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.

8. The organization disables tftp, (trivial ftp); X-Windows, Sun Open Windows; FTP; TELNET; IPX/SPX; NETBIOS; Bluetooth; RPC-services, like NIS or NFS; rlogin, rsh, rexec; SMTP (Simple Mail Transfer Protocol); RIP (Routing Information Protocol); DNS (Domain Name Services); UUCP (Unix- Unix Copy Protocol); NNTP (Network News Transfer Protocol); NTP (Network Time Protocol); Peer-to-Peer except for explicitly identified components in support of specific operational requirements.

   Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	**LOW** AC-17	**MOD** AC-17 (1) (2) (3) (4) (5) (7) (8)	**HIGH** AC-17 (1) (2) (3) (4) (5) (7) (8)

AC-18 WIRELESS ACCESS

Applicability: All Information Systems

Control: The organization:

a. Establishes usage restrictions and implementation guidance for wireless access;
b. Monitors for unauthorized wireless access to the information system;
c. Authorizes wireless access to the information system prior to connection; and
d. Enforces requirements for wireless connections to the information system.

Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization controlled facilities. Related controls: AC-3, IA-2, IA-3, IA-8.

Control Enhancements:

1. The information system protects wireless access to the system using authentication and encryption.

   Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary. Related control: SC-13.

2. The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points quarterly, and takes appropriate action if an unauthorized connection is discovered.

   Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information

systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

3. The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

4. The organization does not allow users to independently configure wireless networking capabilities.

5. The organization confines wireless communications to organization-controlled boundaries.

   Enhancement Supplemental Guidance: Actions that may be taken by the organization to confine wireless communications to organization-controlled boundaries include: (i) reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) configuring the wireless access such that it is point to point in nature.

References: NIST Special Publications 800-48, 800-94, 800-97.

Priority and Baseline Allocation:

P1	**LOW** AC-18	**MOD** AC-18 (1) (2)	**HIGH** AC-18 (1) (2) (3) (4) (5)

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Applicability: All Information Systems

Control: The organization:

a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;
b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;
c. Monitors for unauthorized connections of mobile devices to organizational information systems;
d. Enforces requirements for the connection of mobile devices to organizational information systems;
e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for

example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

Control Enhancements:

1. The organization restricts the use of writable, removable media in organizational information systems.
2. The organization prohibits the use of personally owned, removable media in organizational information systems.
3. The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

   Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

References: NIST Special Publications 800-114, 800-124.

Priority and Baseline Allocation:

P1	**LOW** AC-19	**MOD** AC-19 (1) (2) (3)	**HIGH** AC-19 (1) (2) (3)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Applicability: All Information Systems

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from the external information systems; and
b. Process, store, and/or transmit organization-controlled information using the external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, Smartphones, personal digital assistants or personal electronic devices (PDAs/PEDs), etc.); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.

Control Enhancements:

1. The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
    a. Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
    b. Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

2. The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

    Enhancement Supplemental Guidance: Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

All sensitive agency information, including Personally Identifiable Information (PII), shall only be processed, housed, transmitted or stored using DOI controlled and managed computing and network resources. To clarify, this does not imply that agency employees or contractors are required to use Government Furnished Equipment (GFE) computers or devices as there are many options available within which this requirement can be met. The intent of the requirement is that it is the sensitive information that requires adequate protection and to be able to ensure its protection the agency can only do so by ensuring that it effectively manages the resources that afford such information/data adequate protection. Examples of some options to meet the requirement might include:

- The agency deploying and managing virtualized secured client operating systems on personally owned (non-GFE) computers where the configuration management and control over such virtual environments is managed by the agency while the employee retains control over their own non-virtualized operating system configuration. The virtualized environment should be configured to prevent any sensitive agency information from being saved to, or stored on, the personally owned computer outside of the protected virtual environment and its encrypted data/information storage allocated for use and accessible only by the virtual environment.
- The agency providing technology that includes secure virtualized operating system environments and encrypted storage that resides solely on a security hardened USB Thumb-drive.
- The agency providing approved technology that securely enables remote access of internal agency computer or network resources on which to perform assigned work (e.g., Citrix) that virtualizes user session and prevents downloading, copying, printing, screen capturing, etc. of any data/information locally at the remote location.

Requiring use of only agency GFE computers is an option where the above, or similar secure operating capabilities, are not available or otherwise viable.

Agency employees and contractors are permitted to use their own Internet Service Providers (ISPs) to connect to the agency's approved enterprise remote access solutions that provide encrypted communication tunnels for the secure transport (transmission) of any sensitive agency information between the connecting system and the agency network computing environment. Similarly, agency employees and contractors are permitted to use their home, or other, Wi-Fi connections to establish Internet connectivity and connect to the agency's enterprise remote access solutions provided those connections employ authenticated, encrypted, and secure configurations that are compliant with applicable standards (i.e., the most current versions of NIST FIPS 140, *Security Requirements for Cryptographic Modules*; Best Practice Security Recommendations specified in NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*; NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*; and NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*) to minimize the likelihood that the computing resources they are using are not susceptible to direct attack.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** AC-20	**MOD** AC-20 (1) (2)	**HIGH** AC-20 (1) (2)

AC-22 PUBLICLY ACCESSIBLE CONTENT

Applicability: All Information Systems

Control: The organization:

a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;
d. Reviews the content on the publicly accessible organizational information system for nonpublic information quarterly; and
e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance: Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by appropriate organizational policy. Related controls: AC-3, AU-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** AC-22	**MOD** AC-22	**HIGH** AC-22

Department of the Interior

Security Control Standard

Security Assessment and Authorization

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	December 16, 2010	Initial draft
Timothy Brown	0.2	December 27, 2010	Incorporated comments into text, removed non-mandated control enhancements
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Checked and added cloud requirements for high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012 and alignment to OMB M-11-33 to support ongoing authorizations

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: SECURITY ASSESSMENT AND AUTHORIZATION **5**

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES 5
CA-2 SECURITY ASSESSMENTS 6
CA-3 INFORMATION SYSTEM CONNECTIONS 8
CA-5 PLAN OF ACTION AND MILESTONES 9
CA-6 SECURITY AUTHORIZATION 9
CA-7 CONTINUOUS MONITORING 10

SECURITY CONTROL STANDARD: SECURITY ASSESSMENT AND AUTHORIZATION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Security Assessment and Authorization (CA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security assessment and authorization family. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

Priority and Baseline Allocation:

P1	LOW CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Applicability: All Information Systems

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
   - Security controls and control enhancements under assessment;
   - Assessment procedures to be used to determine security control effectiveness; and
   - Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

Supplemental Guidance: The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by the organization, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should *not* be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical by the organization to protecting organizational operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-6, CA-7, PM-9, SA-11.

Control Enhancements:

1. The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

   Enhancement Supplemental Guidance: An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. The authorizing official determines the required level of assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets, and to individuals. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results.

2. The organization includes an independent penetration test as part of security control assessments, at least annually, for all high impact information systems. Electronic and hard copy reports of penetration test results will be provided to the COR. The government will reserve the right to conduct unannounced and prearranged independent vulnerability scans using government personnel or another contractor.

   Enhancement Supplemental Guidance: Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities.

Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions. Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Testing is conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Testing methods are approved by authorizing officials in coordination with the organization's Risk Executive Function. Vulnerabilities uncovered during red team exercises are incorporated into the vulnerability remediation process. Related controls: RA-5, SI-2.

References: FIPS Publication 199; NIST Special Publications 800-37, 800-53A, 800-115.

Priority and Baseline Allocation:

P2	**LOW** CA-2 (1)	**MOD** CA-2 (1)	**HIGH** CA-2 (1) (2)

CA-3 INFORMATION SYSTEM CONNECTIONS

Applicability: All Information Systems

Control: The organization:

a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;
b. documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

Supplemental Guidance: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or

alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a federal agency and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. Related controls: AC-4, IA-3, SC-7, SA-9.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-47.

Priority and Baseline Allocation:

P1	**LOW** CA-3	**MOD** CA-3	**HIGH** CA-3

CA-5 PLAN OF ACTION AND MILESTONES

Applicability: All Information Systems

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: The plan of action and milestones is a key document in the security authorization package and is subject to federal reporting requirements established by OMB.

Related control: PM-4.

Control Enhancements: None mandated.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	**LOW** CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY AUTHORIZATION

Applicability: All Information Systems

Control: The organization:

a. Assigns a senior-level executive or manager to the role of authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Conducts ongoing security authorization of information systems through the implementation of continuous monitoring programs.

Supplemental Guidance: Security authorization is the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. Rather than enforcing a static three-year reauthorization process, and to reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for the ongoing authorization. In accordance with OMB policy, continuous monitoring programs thus fulfill the three-year security reauthorization requirement eliminating the need for a separate reauthorization process. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements: None.

References: OMB Circular A-130; OMB M-11-33; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	LOW CA-6	MOD CA-6	HIGH CA-6

CA-7 CONTINUOUS MONITORING

Applicability: All Information Systems

Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. A configuration management process for the information system and its constituent components;
b. A determination of the security impact of changes to the information system and environment of operation;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
d. Reporting the security state of the information system to the Authorizing Official at least quarterly.

Supplemental Guidance: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4.

Control Enhancements:

2. The organization plans, schedules, and conducts annual unannounced, penetration testing and in-depth monitoring to ensure compliance with all vulnerability mitigation procedures.

   Enhancement Supplemental Guidance: Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing also provides independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, red-team exercises, and other forms of security testing. Related control: CA-2.

References: NIST Special Publications 800-37, 800-53A; US-CERT Technical Cyber Security Alerts; DOD Information Assurance Vulnerability Alerts.

Priority and Baseline Allocation:

P3	**LOW** CA-7	**MOD** CA-7 (2)	**HIGH** CA-7 (2)

Department of the Interior

Security Control Standard

Audit and Accountability

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	December 8, 2010	Initial draft
Timothy Brown	0.2	December 10, 2010	Incorporated comments into text, removed non-mandated control enhancements
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: AUDIT AND ACCOUNTABILITY **5**

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES 5
AU-2 AUDITABLE EVENTS 6
AU-3 CONTENT OF AUDIT RECORDS 7
AU-4 AUDIT STORAGE CAPACITY 8
AU-5 RESPONSE TO AUDIT PROCESSING FAILURES 8
AU-6 AUDIT REVIEWN, ANALYSIS, AND REPORTING 9
AU-7 AUDIT REDUCTION AND REPORT GENERATION 9
AU-8 TIME STAMPS 10
AU-9 PROTECTION OF AUDIT INFORMATION 10
AU-10 NON-REPUDIATION 10
AU-11 AUDIT RECORD RETENTION 11
AU-12 AUDIT GENERATION 12

SECURITY CONTROL STANDARD: AUDIT AND ACCOUNTABILITY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Audit and Accountability (AU) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the

organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AU-1	MOD AU-1	HIGH AU-1

AU-2 AUDITABLE EVENTS

Applicability: All Information Systems

Control: The organization:

a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;
b. Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].

Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are to be *audited* at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.

Control Enhancements:

3. The organization reviews and updates the list of auditable events annually or whenever there is a change in the threat environment.

Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.

4. The organization includes execution of privileged functions in the list of events to be audited by the information system and configures auditing features of operating systems, databases, and applications to record security-related events, to include logon/logoff and all failed access attempts.

References: NIST Special Publication 800-92.

Priority and Baseline Allocation:

P1	**LOW** AU-2	**MOD** AU-2 (3) (4)	**HIGH** AU-2 (3) (4)

AU-3 CONTENT OF AUDIT RECORDS

Applicability: All Information Systems

Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.

Control Enhancements:

1. The information system includes session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon in the audit records for audit events identified by type, location, or subject.

Enhancement Supplemental Guidance: An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

2. The organization centrally manages the content of audit records generated by individual components throughout the system.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Applicability: All Information Systems

Control: Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Applicability: All Information Systems

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and
b. Takes the following additional actions: overwrite oldest audit records (low impact system); shut down information system (moderate and high impact systems).

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

1. The information system provides a warning when allocated audit record storage volume reaches 75 percent of maximum audit record storage capacity.
2. The information system provides a real-time alert when the following audit failure events occur: any critical device failure; any administrator account failure; all relevant user activity that could lead to an incident or attempted security breach.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT REVIEWN, ANALYSIS, AND REPORTING

Applicability: All Information Systems

Control: The organization:

a. Reviews and analyzes information system audit records *at least weekly* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: Related control: AU-7.

Control Enhancements:

1. The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
3. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-6	**MOD** AU-6 (1) (3)	**HIGH** AU-6 (1) (3)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Applicability: Moderate and High Impact Information Systems

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.

Control Enhancements:

1. The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Applicability: All Information Systems

Control: The information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.

Control Enhancements:

1. The information system synchronizes internal information system clocks at least hourly with a NIST Internet Time Service server.

References: http://tf.nist.gov/tf-cgi/servers.cgi

Priority and Baseline Allocation:

P2	**LOW** AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Applicability: All Information Systems

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.

Control Enhancements:

2. The information system backs up audit records at least weekly onto a different system or media than the system being audited.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-9	**MOD** AU-9 (2)	**HIGH** AU-9 (2)

AU-10 NON-REPUDIATION

Applicability: Moderate and High Impact Information Systems

Control: The information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Control Enhancements:

5. The organization employs FIPS 140-2 validated cryptography to implement digital signatures.

   Enhancement Supplemental Guidance: Related control: SC-13.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AU-10 (5)	HIGH AU-10 (5)

AU-11 AUDIT RECORD RETENTION

Applicability: All Information Systems

Control: The organization retains audit records for 30 days (low impact systems), 60 days (moderate impact systems), or 90 days (high impact systems) to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	LOW AU-11	MOD AU-11	HIGH AU-11

AU-12 AUDIT GENERATION

Applicability: All Information Systems

Control: The information system:

a. Provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed;
b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Supplemental Guidance: Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related controls: AU-2, AU-3.

Control Enhancements:

1. The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

   Enhancement Supplemental Guidance: The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AU-12	**MOD** AU-12	**HIGH** AU-12 (1)

Department of the Interior

Security Control Standard

Awareness and Training

April 2011

Version: 1.1

Attachment 1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	December 2, 2010	Initial draft
Timothy Brown	0.2	December 3, 2010	Incorporated comments into body text
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Checked/added cloud controls to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; remove margin notes
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: AWARENESS AND TRAINING 5

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES 5
AT-2 SECURITY AWARENESS 6
AT-3 SECURITY TRAINING 6
AT-4 SECURITY TRAINING RECORDS 7

SECURITY CONTROL STANDARD: AWARENESS AND TRAINING

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Awareness and Training (AT) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS

Applicability: All Information Systems

Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to the organization's information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Control Enhancements: None mandated.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publication 800-50.

Priority and Baseline Allocation:

P1	LOW AT-2	**MOD** AT-2	**HIGH** AT-2

AT-3 SECURITY TRAINING

Applicability: All Information Systems

Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) at least annually thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program. Related controls: AT-2, SA-3.

Control Enhancements: None.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Applicability: All Information Systems

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for at least 3 years.

Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AT-4	**MOD** AT-4	**HIGH** AT-4

Department of the Interior

Security Control Standard

Configuration Management

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	December 17, 2010	Initial draft
Timothy Brown	0.2	December 27, 2010	Incorporated comments into text, removed non-mandated control enhancements
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes. (several required controls still need defined values)
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: CONFIGURATION MANAGEMENT 5

CM-1 CONFIGURATION MANAGEMENT POLICIES AND PROCEDURES 5
CM-2 BASELINE CONFIGURATION 6
CM-3 CONFIGURATION CHANGE CONTROL 7
CM-4 SECURITY IMPACT ANALYSIS 8
CM-5 ACCESS RESTRICTIONS FOR CHANGE 9
CM-6 CONFIGURATION SETTINGS 10
CM-7 LEAST FUNCTIONALITY 11
CM-8 INFORMATION SYSTEM COMPONENT INVENTORY 12
CM-9 CONFIGURATION MANAGEMENT PLAN 13

SECURITY CONTROL STANDARD: CONFIGURATION MANAGEMENT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Configuration Management (CM) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

CM-1 CONFIGURATION MANAGEMENT POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Applicability: All Information Systems

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9.

Control Enhancements:

1. The organization reviews and updates the baseline configuration of the information system:
   a. Annually;
   b. When required due to a significant change; and
   c. As an integral part of information system component installations and upgrades.

2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

   Enhancement Supplemental Guidance: Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components, mobile devices) and used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can also scan information systems for

unauthorized software to validate organization defined lists of authorized and unauthorized software programs.

3. The organization retains older versions of baseline configurations as deemed necessary to support rollback.

4. The organization:
   a. Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and
   b. Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

5. The organization:
   a. Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and
   b. Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

6. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-2	**MOD** CM-2 (1) (3) (4) (5)	**HIGH** CM-2 (1) (2) (3) (5) (6)

CM-3 CONFIGURATION CHANGE CONTROL

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Determines the types of changes to the information system that are configuration controlled;
b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;
c. Documents approved configuration-controlled changes to the system;
d. Retains and reviews records of configuration-controlled changes to the system;
e. Audits activities associated with configuration-controlled changes to the system; and
f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board)*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Supplemental Guidance: The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology

products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. Related controls: CM-4, CM-5, CM-6, SI-2.

Control Enhancements:

1. The organization employs automated mechanisms to:
   a. Document proposed changes to the information system;
   b. Notify designated approval authorities;
   c. Highlight approvals that have not been received by [*Assignment: organization-defined time period*];
   d. Inhibit change until designated approvals are received; and
   e. Document completed changes to the information system.

2. The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

   Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	LOW Not Selected	**MOD** CM-3 (2)	**HIGH** CM-3 (1) (2)

CM-4 SECURITY IMPACT ANALYSIS

Applicability: All Information Systems

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security

ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-7, CM-3, CM-9, SI-2.

Control Enhancements:

1. The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Enhancement Supplemental Guidance: Changes include information system upgrades and modifications.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P2	**LOW** CM-4	**MOD** CM-4	**HIGH** CM-4 (1)

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Applicability: Moderate and High Impact Information Systems

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
2. The organization conducts audits of information system changes [*Assignment: organization defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred.
3. The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.
5. The organization:
    a. Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and
    b. Reviews and reevaluates information system developer/integrator privileges at least quarterly.

Enhancement Supplemental Guidance: Critical software programs and/or modules include, for example, patches, service packs, and where applicable, device drivers.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-5 (1) (5)	**HIGH** CM-5 (1) (2) (3) (5)

CM-6 CONFIGURATION SETTINGS

Applicability: All Information Systems

a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using United States Government Configuration Baseline checklists that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A *security configuration checklist* (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security

configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: CM-2, CM-3, SI-4.

Control Enhancements:

1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

2. The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

   Enhancement Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.

3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

   Enhancement Supplemental Guidance: Related controls: IR-4, IR-5.

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: NVD.NIST.GOV; WWW.NSA.GOV.

Priority and Baseline Allocation:

P1	**LOW** CM-6	**MOD** CM-6 (1) (3)	**HIGH** CM-6 (1) (2) (3)

CM-7 LEAST FUNCTIONALITY

Applicability: All Information Systems

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services:

- All Unencrypted Network Transactions used for authentication or for any sensitive agency information
- Telnet
- FTP (Unless Approved by OCIO).

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations

limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related control: RA-5.

Control Enhancements:

1. The organization reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services.
2. The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].

   Enhancement Supplemental Guidance: Related control: CM-2.

References: None.

Priority and Baseline Allocation:

P1	LOW CM-7	**MOD** CM-7 (1)	**HIGH** CM-7 (1) (2)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Applicability: All Information Systems

Control: The organization develops, documents, and maintains an inventory of information system components that:

a. Accurately reflects the current information system;
b. Is consistent with the authorization boundary of the information system;
c. Is at the level of granularity deemed necessary for tracking and reporting;
d. Includes manufacturer, model number, serial number, software license information, system/component owner; and
e. Is available for review and audit by designated organizational officials.

Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. Related controls: CM-2, CM-6.

Control Enhancements:

1. The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.
2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

   Enhancement Supplemental Guidance: Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this control enhancement is to maintain as up-to-date, complete, and accurate an inventory as is reasonable.

3. The organization:

   a. Employs automated mechanisms continuously, using automated mechanisms with a maximum five-minute delay in detection, to detect the addition of unauthorized components/devices into the information system; and
   b. Disables network access by such components/devices or notifies designated organizational officials.

   Enhancement Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic scanning of organizational networks for that purpose. Automated mechanisms can be implemented within the information system and/or in another separate information system or device. Related controls: AC-17, AC-19.

4. The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components.

5. The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-8	**MOD** CM-8 (1) (3) (5)	**HIGH** CM-8 (1) (2) (3) (4) (5)

CM-9 CONFIGURATION MANAGEMENT PLAN

Applicability: Moderate and High Impact Information Systems

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and
c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Supplemental Guidance: Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. Related control: SA-10.

Control Enhancements: None mandated.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-9	**HIGH** CM-9

Department of the Interior

Security Control Standard

Contingency Planning

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 7, 2011	Initial draft
Timothy Brown	0.2	January 11, 2011	Cover page, incorporated comments into body text
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes. Retained margin notes re: "cloud service provider" and reviewer comment/recommendations
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: CONTINGENCY PLANNING 5

CP-1 CONTINGENCY PLANNING POLICIES AND PROCEDURES 5
CP-2 CONTINGENCY PLAN 6
CP-3 CONTINGENCY TRAINING 7
CP-4 CONTINGENCY PLAN TESTING AND EXERCISES 8
CP-6 ALTERNATE STORAGE SITE 9
CP-7 ALTERNATE PROCESSING SITE 9
CP-8 TELECOMMUNICATIONS SERVICES 10
CP-9 INFORMATION SYSTEM BACKUP 11
CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION 12

SECURITY CONTROL STANDARD: CONTINGENCY PLANNING

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Contingency Planning (CP) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

CP-1 CONTINGENCY PLANNING POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. Related control: PM-9.

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Applicability: All Information Systems

Control: The organization:

a. Develops a contingency plan for the information system that:
   - Identifies essential missions and business functions and associated contingency requirements;
   - Provides recovery objectives, restoration priorities, and metrics;
   - Addresses contingency roles, responsibilities, assigned individuals with contact information;
   - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
   - Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*];
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system at least annually;
e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and
f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the

confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.

Control Enhancements:

1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

   Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-2	**MOD** CP-2 (1) (2)	**HIGH** CP-2 (1) (2) (3)

CP-3 CONTINGENCY TRAINING

Applicability: All Information Systems

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at least annually.

Supplemental Guidance: None.

Control Enhancements:

1. The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** CP-3	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Applicability: All Information Systems

Control: The organization:

a. Tests and/or exercises the contingency plan for the information system at least annually using functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems to determine the plan's effectiveness and the organization's readiness to execute the plan; and
b. Reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

Control Enhancements:

1. The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

   Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

2. The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

4. The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

   Enhancement Supplemental Guidance: Related controls: CP-10, SC-24.

References: FIPS Publication 199; NIST Special Publications 800-34, 800-84.

Priority and Baseline Allocation:

P2	**LOW** CP-4	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2) (4)

CP-6 ALTERNATE STORAGE SITE

Applicability: Moderate and High Impact Systems

Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.

Control Enhancements:

1. The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.

   Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.

2. The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

3. The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

   Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CP-6 (1) (3)	HIGH CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Applicability: Moderate and High Impact Systems

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within timeframes compliant with the Business Impact Analysis for the system, but no later than 90 days when the primary processing capabilities are unavailable; and
b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

1. The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

   Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.

2. The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

3. The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

4. The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.

5. The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-7 (1) (2) (3) (5)	**HIGH** CP-7 (1) (2) (3) (4) (5)

CP-8 TELECOMMUNICATIONS SERVICES

Applicability: Moderate and High Impact Systems

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within 90 days when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

1. The organization:
   a. Develops primary and alternate telecommunications service agreements that contain priority of-service provisions in accordance with the organization's availability requirements; and
   b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.
2. The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

3. The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.
4. The organization requires primary and alternate telecommunications service providers to have contingency plans.

References: NIST Special Publication 800-34; Web: TSP.NCS.GOV.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD CP-8 (1) (2)	HIGH CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Applicability: All Information Systems

Control: The organization:

a. Conducts backups of user-level information contained in the information system at least daily incremental and weekly full;
b. Conducts backups of system-level information contained in the information system at least daily incremental and weekly full;
c. Conducts backups of information system documentation including security-related documentation at least daily incremental and weekly full; and
d. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.

Control Enhancements:

1. The organization tests backup information at least annually to verify media reliability and information integrity.
2. The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.
3. The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	LOW CP-9	MOD CP-9 (1) (3)	HIGH CP-9 (1) (2) (3)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Applicability: All Information Systems

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, SC-24.

Control Enhancements:

2. The information system implements transaction recovery for systems that are transaction-based.

   Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

3. The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*].
4. The organization provides the capability to reimage information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-10	**MOD** CP-10 (2) (3)	**HIGH** CP-10 (2) (3) (4)

Department of the Interior

Security Control Standard

Identification and Authentication

January 2012

Version: 1.4

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 10, 2011	Initial draft
Timothy Brown	0.2	January 12, 2010	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes. Retained margin notes re: "service provider" and/or "Joint Approval Board (JAB)"
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	May 10, 2011	Incorporated recommended changes to IA-5
Lawrence K. Ruffin	1.3	July 26, 2011	Modified the IA-5 Control Enhancement 1 language in the Enhancement Supplemental Guidance to eliminate specific reference to AES 256 to instead require NIST FIPS 140-2 compliant/validated cryptographic modules
Lawrence K. Ruffin	1.4	January 18, 2012	Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: IDENTIFICATION AND AUTHENTICATION **5**

IA-1 IDENTIFICATION AND AUTHENTICATION POLICIES AND PROCEDURES 5
IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) 6
IA-3 DEVICE IDENTIFICATION AND AUTHENICATION 7
IA-4 IDENTIFIER MANAGEMENT 8
IA-5 AUTHENTICATOR MANAGMENT 8
IA-6 AUTHENTICATOR FEEDBACK 11
IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION 11
IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) 11

SECURITY CONTROL STANDARD: IDENTIFICATION AND AUTHENTICATION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Identification and Authentication (IA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

IA-1 IDENTIFICATION AND AUTHENTICATION POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary.

The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Priority and Baseline Allocation:

P1	LOW IA-1	MOD IA-1	HIGH IA-1

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Applicability: All Information Systems

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8. The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.

Control Enhancements:

1. The information system uses multifactor authentication for network access to privileged accounts.
2. The information system uses multifactor authentication for network access to non-privileged accounts.
3. The information system uses multifactor authentication for local access to privileged accounts.
4. The information system uses multifactor authentication for local access to non-privileged accounts.
8. The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.

   Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators. The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to non-privileged accounts.

9. The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to non-privileged accounts.

   Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

References: HSPD 12; OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-2 (1)	**MOD** IA-2 (1) (2) (3) (8)	**HIGH** IA-2 (1) (2) (3) (4) (8) (9)

IA-3 DEVICE IDENTIFICATION AND AUTHENICATION

Applicability: Moderate and High Impact Information Systems

Control: The information system uniquely identifies and authenticates [*Assignment: organization defined list of specific and/or types of devices*] before establishing a connection.

Supplemental Guidance: The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD IA-3	HIGH IA-3

IA-4 IDENTIFIER MANAGEMENT

Applicability: All Information Systems

Control: The organization manages information system identifiers for users and devices by:

a. Receiving authorization from a designated organizational official to assign a user or device identifier;
b. Selecting an identifier that uniquely identifies an individual or device;
c. Assigning the user identifier to the intended party or the device identifier to the intended device;
d. Preventing reuse of user or device identifiers for at least two years; and
e. Disabling the user identifier after 90 days of inactivity.

Supplemental Guidance: Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related control: AC-2, IA-2.

Control Enhancements:

4. The organization manages user identifiers by uniquely identifying the user as contractors; foreign nationals.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	LOW IA-4	MOD IA-4 (4)	HIGH IA-4 (4)

IA-5 AUTHENTICATOR MANAGMENT

Applicability: All Information Systems

Control: The organization manages information system authenticators for users and devices by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators upon information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
g. Changing/refreshing authenticators at least every 60 days, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices), but not greater than 90 days;
h. Protecting authenticator content from unauthorized disclosure and modification; and
i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.

Control Enhancements:

1. The information system, for password-based authentication:
    a. Enforces minimum password complexity of 12 or more case sensitive characters, with a minimum of one character from at least three of the following four categories: uppercase, lowercase, numeric, and special (non-alphanumeric); unless other acceptable complexity rules or pattern checks are specified and allowed to be less complex by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices).
    b. Enforces at least one changed character when new passwords are created;
    c. Encrypts passwords in storage and in transmission;
    d. Enforces password minimum and maximum lifetime restrictions of one day minimum; and 60 day maximum, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal

Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices), but not greater than 90 days; and

e. Prohibits password reuse for 24 generations.

Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

Mobile devices, configured with content protection enabled using NIST FIPS 140-2 compliant/validated cryptographic modules and to automatically wipe all data after ten failed login attempts, may use strong passwords with as few as six (6) characters having at least one uppercase, lowercase, and numeric; and a minimum password age of 1 day and a maximum of 90 days. Mobile devices include Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices, but does not include portable laptop computers.

2. The information system, for PKI-based authentication:
   a. Validates certificates by constructing a certification path with status information to an accepted trust anchor;
   b. Enforces authorized access to the corresponding private key; and
   c. Maps the authenticated identity to the user account.

   Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

3. The organization requires that the registration process to receive HSPD12 smart cards shall be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

6. The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.

7. The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

   Enhancement Supplemental Guidance: Organizations exercise caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

References: OMB Memorandums 04-04, 06-16, 07-16; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78; NIST Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB).

Priority and Baseline Allocation:

P1	**LOW** IA-5 (1)	**MOD** IA-5 (1) (2) (3) (6) (7)	**HIGH** IA-5 (1) (2) (3) (6) (7)

IA-6 AUTHENTICATOR FEEDBACK

Applicability: All Information Systems

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

Control Enhancements: None.

References: None

Priority and Baseline Allocation:

P1	**LOW** IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Applicability: All Information Systems

Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Supplemental Guidance: None.

Control Enhancements: None.

References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL.

Priority and Baseline Allocation:

P1	**LOW** IA-7	**MOD** IA-7	**HIGH** IA-7

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Applicability: All Information Systems

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related controls: AC-14, AC-17, AC-18, MA-4.

Control Enhancements: None.

References: OMB Memorandum 04-04; Web: WWW.CIO.GOV/EAUTHENTICATION; NIST Special Publication 800-63.

Priority and Baseline Allocation:

P1	**LOW** IA-8	**MOD** IA-8	**HIGH** IA-8

Department of the Interior

Security Control Standard

Incident Response

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 13, 2011	Initial draft
Timothy Brown	0.2	January 20, 2011	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes. Retained notes re: "service provider" and/or Joint Authorization Board (JAB)
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: INCIDENT RESPONSE **5**

IR-1 INCIDENT RESPONSE POLICIES AND PROCEDURES 5
IR-2 INCIDENT RESPONSE TRAINING 6
IR-3 INCIDENT RESPONSE TESTING AND EXERCISES 6
IR-4 INCIDENT HANDLING 7
IR-5 INCIDENT MONITORING 8
IR-6 INCIDENT REPORTING 8
IR-7 INCIDENT RESPONSE ASSISTANCE 9
IR-8 INCIDENT RESPONSE PLAN 10

SECURITY CONTROL STANDARD: INCIDENT RESPONSE

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Incident Response (IR) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

IR-1 INCIDENT RESPONSE POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Priority and Baseline Allocation:

P1	LOW IR-1	MOD IR-1	HIGH IR-1

IR-2 INCIDENT RESPONSE TRAINING

Applicability: All Information Systems

Control: The organization:

a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training at least annually.

Supplemental Guidance: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.

Control Enhancements:

1. The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
2. The organization employs automated mechanisms to provide a more thorough and realistic training environment.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	LOW IR-2	MOD IR-2	HIGH IR-2 (1) (2)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Applicability: Moderate and High Impact Information Systems

Control: The organization tests and/or exercises the incident response capability for the information system at least annually using tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended) to determine the incident response effectiveness and documents the results.

Supplemental Guidance: None.

Control Enhancements:

1. The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

   Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability. Related control: AT-2.

References: NIST Special Publications 800-84, 800-115.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD IR-3	HIGH IR-3 (1)

IR-4 INCIDENT HANDLING

Applicability: All Information Systems

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

1. The organization employs automated mechanisms to support the incident handling process.

   Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	LOW IR-4	MOD IR-4 (1)	HIGH IR-4 (1)

IR-5 INCIDENT MONITORING

Applicability: All Information Systems

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Control Enhancements:

1. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

   Enhancement Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-6, AU-7, SI-4.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-5	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Applicability: All Information Systems

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended) ; and
b. Reports security incident information to designated authorities.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time

frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5.

Control Enhancements:

1. The organization employs automated mechanisms to assist in the reporting of security incidents.

References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.

Priority and Baseline Allocation:

P1	**LOW** IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Applicability: All Information Systems

Control: The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.

Control Enhancements:

1. The organization employs automated mechanisms to increase the availability of incident response-related information and support.

   Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

2. The organization:

   a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
   b. Identifies organizational incident response team members to the external providers.

Enhancement Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

References: None.

Priority and Baseline Allocation:

P3	LOW IR-7	MOD IR-7 (1) (2)	HIGH IR-7 (1) (2)

IR-8 INCIDENT RESPONSE PLAN

Applicability: All Information Systems

Control: The organization:

a. Develops an incident response plan that:
   - Provides the organization with a roadmap for implementing its incident response capability;
   - Describes the structure and organization of the incident response capability;
   - Provides a high-level approach for how the incident response capability fits into the overall organization;
   - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   - Defines reportable incidents;
   - Provides metrics for measuring the incident response capability within the organization;
   - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   - Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*];
c. Reviews the incident response plan at least annually;
d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

Control Enhancements: None.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	LOW IR-8	MOD IR-8	HIGH IR-8

Department of the Interior

Security Control Standard

Maintenance

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 14, 2011	Initial draft
Timothy Brown	0.2	January 20, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Incorporated the additional MA-5 control enhancements applicable to all Moderate and High systems

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: MAINTENANCE **5**

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES 5
MA-2 CONTROLLED MAINTENANCE 6
MA-3 MAINTENANCE TOOLS 7
MA-4 NON-LOCAL MAINTENANCE 7
MA-5 MAINTENANCE PERSONNEL 8
MA-6 TIMELY MAINTENANCE 10

SECURITY CONTROL STANDARD: MAINTENANCE

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Maintenance (MA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in

general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW MA-1	MOD MA-1	HIGH MA-1

MA-2 CONTROLLED MAINTENANCE

Applicability: All Information Systems

Control: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Supplemental Guidance: The control is intended to address the information security aspects of the organization's information system maintenance program. Related controls: MP-6, SI-2.

Control Enhancements:

1. The organization maintains maintenance records for the information system that include:
    a. Date and time of maintenance;
    b. Name of the individual performing the maintenance;
    c. Name of escort, if necessary;
    d. A description of the maintenance performed; and
    e. A list of equipment removed or replaced (including identification numbers, if applicable).

2. The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

References: None.

Priority and Baseline Allocation:

P2	LOW MA-2	MOD MA-2 (1)	HIGH MA-2 (1) (2)

MA-3 MAINTENANCE TOOLS

Applicability: Moderate and High Impact Information Systems

Control: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

Supplemental Guidance: The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. Related control: MP-6.

Control Enhancements:

1. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

   Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

2. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

3. The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

References: NIST Special Publication 800-88.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MA-3 (1) (2) (3)	HIGH MA-3 (1) (2) (3)

MA-4 NON-LOCAL MAINTENANCE

Applicability: All Information Systems

Control: The organization:

a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities;

b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintains records for non-local maintenance and diagnostic activities; and
e. Terminates all sessions and network connections when non-local maintenance is completed.

Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part, by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

Control Enhancements:

1. The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.
2. The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.
3. The organization:
    a. Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or
    b. Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

P1	LOW MA-4	MOD MA-4 (1) (2)	HIGH MA-4 (1) (2) (3)

MA-5 MAINTENANCE PERSONNEL

Applicability: All Information Systems

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and

b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

Supplemental Guidance: Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.

Control Enhancements:

1. The organization maintains procedures for the use of maintenance personnel that lack appropriate background investigations and security clearances or are not U.S. citizens, that include the following requirements:

    a. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

    b. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

    c. In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.

    Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any Controlled Unclassified Information (CUI); information subject to the Privacy Act, including Personally Identifiable Information (PII); or any other sensitive agency information contained on the information system. Procedures for the use of maintenance personnel shall be documented in the security plan for the information system.

2. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are cleared (i.e., possess appropriate background investigations and security clearances) for the highest level of information on the system.

3. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are U.S. citizens.

References: None.

Priority and Baseline Allocation:

P1	**LOW** MA-5	**MOD** MA-5 (1) (2) (3)	**HIGH** MA-5 (1) (2) (3)

MA-6 TIMELY MAINTENANCE

Applicability: Moderate and High Impact Information Systems

Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within the time periods defined in accordance with the contingency plan and business impact analysis for the information system.

Supplemental Guidance: The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems. Related control: CP-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MA-6	**HIGH** MA-6

Department of the Interior

Security Control Standard

Media Protection

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 19, 2011	Initial draft
Timothy Brown	0.2	January 25, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: MEDIA PROTECTION 5

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES 5
MP-2 MEDIA ACCESS 6
MP-3 MEDIA MARKING 6
MP-4 MEDIA STORAGE 7
MP-5 MEDIA TRANSPORT 8
MP-6 MEDIA SANITATION 10

SECURITY CONTROL STANDARD: MEDIA PROTECTION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Media Protection (MP) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.
Priority and Baseline Allocation:

P1	**LOW** MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Applicability: All Information Systems

Control: The organization restricts access to all information system media to authorized individuals using [*Assignment: organization-defined security measures*].

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related controls: MP-4, PE-3.

Control Enhancements:

1. The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

   Enhancement Supplemental Guidance: This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	**LOW** MP-2	**MOD** MP-2 (1)	**HIGH** MP-2 (1)

MP-3 MEDIA MARKING

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within any area or space for which the bureau or office has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information systems.

Supplemental Guidance: The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations, however, may require markings for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-3	**HIGH** MP-3

MP-4 MEDIA STORAGE

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Physically controls and securely stores magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within [*Assignment: organization-defined controlled areas*] using encryption utilizing a FIPS 140-2 validated encryption module for digital media or secure storage in locked cabinets or safes for non-digital media;
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are also considered

information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting the information and/or information system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. Related controls: AC-3, AC-19, CP-6, CP-9, MP-2, PE-3.

Control Enhancements:

1. The organization employs cryptographic mechanisms to protect information in storage.

Enhancement Supplemental Guidance: Related control: SC-13.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-4 (1)	HIGH MP-4 (1)

MP-5 MEDIA TRANSPORT

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks during transport outside of controlled areas using encryption utilizing a FIPS 140-2 validated encryption module to protect sensitive information residing on digital media;
b. Maintains accountability for information system media during transport outside of controlled areas; and
c. Restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Related controls: AC-19, CP-9.

Control Enhancements:

2. The organization documents activities associated with the transport of information system media.

   Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.

3. The organization employs an identified custodian throughout the transport of information system media.

   Enhancement Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

4. The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

   Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones). Related control: MP-4. Related controls: MP-2; SC-13.

References: FIPS Publication 199; NIST Special Publication 800-60.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-5 (2) (4)	HIGH MP-5 (2) (3) (4)

MP-6 MEDIA SANITATION

Applicability: All Information Systems

Control: The organization:

a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Supplemental Guidance: This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposal.

Control Enhancements:

1. The organization tracks, documents, and verifies media sanitization and disposal actions.
2. The organization tests sanitization equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].
3. The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].

   Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks. Organizations consider sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the organization loses a positive chain of custody for the device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process. Related control: SI-3.

4. The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.
5. The organization sanitizes information system media containing classified information in accordance with NSA standards and policies.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: WWW.NSA.GOV/IA/GUIDANCE/MEDIA_DESTRUCTION_GUIDANCE/INDEX.SHTML.

Priority and Baseline Allocation:

P1	**LOW** MP-6	**MOD** MP-6 (4)	**HIGH** MP-6 (1) (2) (3) (4) (5)

Department of the Interior

Security Control Standard

Personnel Security

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 24, 2011	Initial draft
Timothy Brown	0.2	January 25, 2011	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked cloud mandated controls
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY **3**

TABLE OF CONTENTS **4**

SECURITY CONTROL STANDARD: PERSONNEL SECURITY **5**

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES 5
PS-2 POSITION CATEGORIZATION 6
PS-3 PERSONNEL SCREENING 6
PS-4 PERSONNEL TERMINATION 7
PS-5 PERSONNEL TRANSFER 7
PS-6 ACCESS AGREEMENTS 8
PS-7 THIRD-PARTY PERSONNEL SECURITY 8
PS-8 PERSONNEL SANCTIONS 9

SECURITY CONTROL STANDARD: PERSONNEL SECURITY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Personnel Security (PS) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.
Priority and Baseline Allocation:

P1	**LOW** PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Applicability: All Information Systems

Control: The organization:

a. Assigns a risk designation to all positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position risk designations at least every three years.

Supplemental Guidance: Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

Control Enhancements: None.

References: 5 CFR 731.106(a).

Priority and Baseline Allocation:

P1	**LOW** PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Applicability: All Information Systems

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to the following schedule: for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions.

Supplemental Guidance: Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.

Control Enhancements: None Mandated.

References: 5 CFR 731.106; FIPS Publications 199, 201; NIST Special Publications 800-73, 800-76, 800-78; ICD 704.

Priority and Baseline Allocation:

P1	**LOW** PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Applicability: All Information Systems

Control: The organization, upon termination of individual employment:

a. Terminates information system access;
b. Conducts exit interviews;
c. Retrieves all security-related organizational information system-related property; and
d. Retains access to organizational information and information systems formerly controlled by terminated individual.

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Applicability: All Information Systems

Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within five days.

Supplemental Guidance: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Applicability: All Information Systems

Control: The organization:

a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and
b. Reviews/updates the access agreements at least annually.

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Applicability: All Information Systems

Control: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Documents personnel security requirements; and
c. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents.

Control Enhancements: None.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Applicability: All Information Systems

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization. Related controls: PL-4, PS-6.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-8	**MOD** PS-8	**HIGH** PS-8

Department of the Interior

Security Control Standard

Physical and Environmental Protection

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 21, 2011	Initial draft
Timothy Brown	0.2	January 25, 2011	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked/added cloud moderate to high
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: PHYSICAL AND ENVIRONMENTAL PROTECTION 5

PE-1 PHYSICAL AND ENVIRONMENTAL POLICY AND PROCEDURES 5
PE-2 PHYSICAL ACCESS AUTHORIZATIONS 6
PE-3 PHYSICAL ACCESS CONTROL 7
PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM 8
PE-5 ACCESS CONTROL FOR OUTPUT DEVICES 8
PE-6 MONITORING PHYSICAL ACCESS 9
PE-7 VISITOR CONTROL 9
PE-8 ACCESS RECORDS 10
PE-9 POWER EQUIPMENT AND POWER CABLING 10
PE-10 EMERGENCY SHUTOFF 10
PE-11 EMERGENCY POWER 11
PE-12 EMERGENCY LIGHTING 12
PE-13 FIRE PROTECTION 12
PE-14 TEMPERATURE AND HUMIDITY CONTROLS 13
PE-15 WATER DAMAGE PROTECTION 13
PE-16 DELIVERY AND REMOVAL 14
PE-17 ALTERNATE WORK SITE 14
PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS 15

SECURITY CONTROL STANDARD: PHYSICAL AND ENVIRONMENTAL PROTECTION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Physical and Environmental Protection (PE) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

PE-1 PHYSICAL AND ENVIRONMENTAL POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information

security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Applicability: All Information Systems

Control: The organization:

a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.

Control Enhancements:

1. The organization authorizes physical access to the facility where the information system resides based on position or role.

References: None.

Priority and Baseline Allocation:

P1	LOW PE-2	**MOD** PE-2	**HIGH** PE-2 (1)

PE-3 PHYSICAL ACCESS CONTROL

Applicability: All Information Systems

Control: The organization:

a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verifies individual access authorizations before granting access to the facility;
c. Controls entry to the facility containing the information system using physical access devices and/or guards;
d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices at least annually; and
g. Changes combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Related controls: MP-2, MP-4, PE-2.

Control Enhancements:

1. The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

   Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. See also PS-3, security requirements for personnel access to SCI.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78; ICD 704; DCID 6/9.

Priority and Baseline Allocation:

P1	LOW PE-3	**MOD** PE-3	**HIGH** PE-3(1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Applicability: Moderate and High Impact Information Systems

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD PE-4	HIGH PE-4

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Applicability: Moderate and High Impact Information Systems

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Monitors, printers, and audio devices are examples of information system output devices.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD PE-5	HIGH PE-5

PE-6 MONITORING PHYSICAL ACCESS

Applicability: All Information Systems

Control: The organization:

a. Monitors physical access to the information system to detect and respond to physical security incidents;
b. Reviews physical access logs at least semi-annually; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

Control Enhancements:

1. The organization monitors real-time physical intrusion alarms and surveillance equipment.
2. The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (2)

PE-7 VISITOR CONTROL

Applicability: All Information Systems

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

Control Enhancements:

1. The organization escorts visitors and monitors visitor activity, when required.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-7	**MOD** PE-7 (1)	**HIGH** PE-7 (1)

PE-8 ACCESS RECORDS

Applicability: All Information Systems

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and
b. Reviews visitor access records at least monthly.

Supplemental Guidance: Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.

Control Enhancements:

1. The organization employs automated mechanisms to facilitate the maintenance and review of access records.
2. The organization maintains a record of all physical access, both visitor and authorized individuals.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-8	**MOD** PE-8	**HIGH** PE-8 (1) (2)

PE-9 POWER EQUIPMENT AND POWER CABLING

Applicability: Moderate and High Impact Information Systems

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements: None mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

Control Enhancements: None

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-10	**HIGH** PE-10

PE-11 EMERGENCY POWER

Applicability: Moderate and High Impact Information Systems

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Enhancement Supplemental Guidance: Long-term alternate power supplies for the information system are either manually or automatically activated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Applicability: All Information Systems

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Applicability: All Information Systems

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.
2. The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.
3. The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-13	**MOD** PE-13 (1) (2) (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Applicability: All Information Systems

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled *Thermal Guidelines for Data Processing Environments*; and
b. Monitors temperature and humidity levels continuously.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

References: None.

Priority and Baseline Allocation:

P1	LOW PE-14	**MOD** PE-14	**HIGH** PE-14 (1)

PE-15 WATER DAMAGE PROTECTION

Applicability: All Information Systems

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

References: None.

Priority and Baseline Allocation:

P1	LOW PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Applicability: All Information Systems

Control: The organization authorizes, monitors, and controls all information system components entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW PE-16	MOD PE-16	HIGH PE-16

PE-17 ALTERNATE WORK SITE

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Employs appropriate management, operational, and technical information system security controls at alternate work sites in accordance with the DOI Telework Policy at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

Control Enhancements: None.

References: NIST Special Publication 800-46.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD PE-17	HIGH PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Applicability: Moderate and High Impact Information Systems

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

1. The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-18	**HIGH** PE-18 (1)

Department of the Interior

Security Control Standard

Planning

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 24, 2011	Initial draft
Timothy Brown	0.2	January 26, 2011	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked cloud mandated controls
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: PLANNING 5

PL-1 SECURITY PLANNING POLICY AND PROCEDURES 5
PL-2 SYSTEM SECURITY PLAN 6
PL-4 RULES OF BEHAVIOR 7
PL-5 PRIVACY IMPACT ASSESSMENT 7
PL-6 SECURITY-RELATED ACTIVITY PLANNING 8

SECURITY CONTROL STANDARD: PLANNING

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Planning (PL) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information

system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-18, 800-100.

Priority and Baseline Allocation:

P1	LOW PL-1	MOD PL-1	HIGH PL-1

PL-2 SYSTEM SECURITY PLAN

Applicability: All Information Systems

Control: The organization:

a. Develops a security plan for the information system that:
   - Is consistent with the organization's enterprise architecture;
   - Explicitly defines the authorization boundary for the system;
   - Describes the operational context of the information system in terms of missions and business processes;
   - Provides the security categorization of the information system including supporting rationale;
   - Describes the operational environment for the information system;
   - Describes relationships with or connections to other information systems;
   - Provides an overview of the security requirements for the system;
   - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Reviews the security plan for the information system at least annually; and
c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Related controls: PM-1, PM-7, PM-8, PM-9, PM-11.

Control Enhancements:

2. The organization develops a functional architecture for the information system that identifies and maintains:
   a. External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;
   b. User roles and the access privileges assigned to each role;
   c. Unique security requirements;

d. Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and
e. Restoration priority of information or information system services.

Enhancement Supplemental Guidance: Unique security requirements for the information system include, for example, encryption of key data elements at rest. Specific protection needs for the information system include, for example, the Privacy Act and Health Insurance Portability and Accountability Act.

References: NIST Special Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-2	**MOD** PL-2	**HIGH** PL-2 (2)

PL-4 RULES OF BEHAVIOR

Applicability: All Information Systems

Control: The organization:

a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and
b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior. Related control: PS-6.

Control Enhancements: None Mandated.

References: NIST Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Applicability: All Information Systems

Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

Supplemental Guidance: None.

Control Enhancements: None.

References: OMB Memorandum 03-22.

Priority and Baseline Allocation:

P1	**LOW** PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Applicability: Moderate and High Impact Information Systems

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PL-6	**HIGH** PL-6

Department of the Interior

Security Control Standard

Program Management

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Timothy Brown	0.1	February 09, 2011	Initial draft
Louis Eichenbaum	1.0	February 23, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: PROGRAM MANAGEMENT 5

PM-1 INFORMATION SECURITY PROGRAM PLAN 5
PM-2 SENIOR INFORMATION SECURITY OFFICER 6
PM-3 INFORMATION SECURITY RESOURCES 7
PM-4 PLAN OF ACTION AND MILESTONES PROCESS 7
PM-5 INFORMATION SYSTEM INVENTORY 7
PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE 8
PM-7 ENTERPRISE ARCHITECTURE 8
PM-8 CRITICAL INFRASTRUCTURE PLAN 8
PM-9 RISK MANAGEMENT STRATEGY 9
PM-10 SECURITY AUTHORIZATION PROCESS 9
PM-11 MISSION/BUSINESS PROCESS DEFINITION 10

SECURITY CONTROL STANDARD: PROGRAM MANAGEMENT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Program Management (PM) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

PM-1 INFORMATION SECURITY PROGRAM PLAN

Applicability: Bureaus and Offices

Control: The organization:

a. Develops and disseminates an organization-wide information security program plan that:

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
- Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

- Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Reviews the organization-wide information security program plan at least annually; and

c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Supplemental Guidance: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Control Enhancements: None.

References: None.

PM-2 SENIOR INFORMATION SECURITY OFFICER

Applicability: Bureaus and Offices

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this organizational official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

References: None.

PM-3 INFORMATION SECURITY RESOURCES

Applicability: Bureaus and Offices

Control: The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Applicability: Bureaus and Offices

Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Control Enhancements: None.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

PM-5 INFORMATION SYSTEM INVENTORY

Applicability: Bureaus and Offices

Control: The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.

Control Enhancements: None.

References: None.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Applicability: Bureaus and Offices

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Control Enhancements: None.

References: NIST Special Publication 800-55.

PM-7 ENTERPRISE ARCHITECTURE

Applicability: Bureaus and Offices

Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PM-11, RA-2.

Control Enhancements: None.

References: NIST Special Publication 800-39; Web: WWW.FSAM.GOV.

PM-8 CRITICAL INFRASTRUCTURE PLAN

Applicability: Bureaus and Offices

Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

References: HSPD 7.

PM-9 RISK MANAGEMENT STRATEGY

Applicability: Bureaus and Offices

Control: The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and

b. Implements that strategy consistently across the organization.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Control Enhancements: None.

References: NIST Special Publications 800-30, 800-39.

PM-10 SECURITY AUTHORIZATION PROCESS

Applicability: Bureaus and Offices

Control: The organization:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;

b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Applicability: Bureaus and Offices

Control: The organization:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60.

Department of the Interior

Security Control Standard

Risk Assessment

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 25, 2011	Initial draft
Timothy Brown	0.2	January 28, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: RISK ASSESSMENT 5

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES 5
RA-2 SECURITY CATEGORIZATION 6
RA-3 RISK ASSESSMENT 6
RA-5 VULNERABILITY SCANNING 7

SECURITY CONTROL STANDARD: RISK ASSESSMENT

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Risk Assessment (RA) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually.

a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30,800-100.

Priority and Baseline Allocation:

P1	LOW RA-1	MOD RA-1	HIGH RA-1

RA-2 SECURITY CATEGORIZATION

Applicability: All Information Systems

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owner, mission owners, and information owners/stewards. The organization also considers potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts in categorizing the information system. The security categorization process facilitates the creation of an *inventory* of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. Related controls: CM-8, MP-4, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	LOW RA-2	MOD RA-2	HIGH RA-2

RA-3 RISK ASSESSMENT

Applicability: All Information Systems

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in a security assessment report;
c. Reviews risk assessment results at least every three years or when a significant change occurs; and
d. Updates the risk assessment at least every three years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.

Risk assessments (either formal or informal) can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially *implemented* prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.

Control Enhancements: None.

References: NIST Special Publication 800-30. NIST Special Publication 800-37, Revision 1, Appendix F

Priority and Baseline Allocation:

P1	**LOW** RA-3	**MOD** RA-3	**HIGH** RA-3

RA-5 VULNERABILITY SCANNING

Applicability: All Information Systems

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications quarterly for operating system(s), web application(s), and database(s) (as applicable) and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
   - Enumerating platforms, software flaws, and improper configurations;
   - Formatting and making transparent, checklists and test procedures; and
   - Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities within thirty days for high-risk vulnerabilities ; within ninety days for moderate risk vulnerabilities in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan. Related controls: CA-2, CM-6, RA-3, SI-2.

Control Enhancements:

1. The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.
2. The organization updates the list of information system vulnerabilities scanned monthly or when new vulnerabilities are identified and reported.
3. The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).
4. The organization attempts to discern what information about the information system is discoverable by adversaries.
5. The organization includes privileged access authorization to [*Assignment: organization-identified information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning.
6. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.
7. The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.
9. The organization employs an independent penetration agent or penetration team to:
   a. Conduct a vulnerability analysis on the information system; and
   b. Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

Enhancement Supplemental Guidance: A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario.

References: NIST Special Publications 800-40, 800-70, 800-115; Web: CWE.MITRE.ORG; NVD.NIST.GOV.

Priority and Baseline Allocation:

P1	**LOW** RA-5	**MOD** RA-5 (1) (2) (3) (6) (9)	**HIGH** RA-5 (1) (2) (3) (4) (5) (6) (7) (9)

Department of the Interior

Security Control Standard

System and Communications Protection

January 2012

Version: 1.2

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	February 3, 2011	Initial draft
Timothy Brown	0.2	February 4, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revised SC-13 to require control enhancement 1 for all information systems

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: SYSTEM AND COMMUNICATIONS PROTECTION 5

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES 5
SC-2 APPLICATION PARTITIONING 6
SC-3 SECURITY FUNCTION ISOLATION 6
SC-4 INFORMATION IN SHARED RESOURCES 7
SC-5 DENIAL OF SERVICE PROTECTION 7
SC-6 RESOURCE PRIORITY 8
SC-7 BOUNDARY PROTECTION 8
SC-8 TRANSMISSION INTEGRITY 11
SC-9 TRANSMISSION CONFIDENTIALITY 11
SC-10 NETWORK DISCONNECT 12
SC-11 TRUSTED PATH 12
SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT 13
SC-13 USE OF CRYPTOGRAPHY 13
SC-14 PUBLIC ACCESS PROTECTIONS 14
SC-15 COLLABORATIVE COMPUTING DEVICES 14
SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES 15
SC-18 MOBILE CODE 15
SC-19 VOICE OVER INTERNET PROTOCOL 16
SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUHTORITATIVE SOURCE) 16
SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) 17
SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE 17
SC-23 SESSION AUTHENTICITY 18
SC-24 FAIL IN KNOWN STATE 18
SC-25 THIN NODES 19
SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS 19
SC-28 PROTECTION OF INFORMATION AT REST 20
SC-30 VIRTUALIZATION TECHNIQUES 20
SC-32 INFORMATION SYSTEM PARTITIONING 21
SC-33 TRANSMISSION PREPARATION INTEGRITY 21

SECURITY CONTROL STANDARD: SYSTEM AND COMMUNICATIONS PROTECTION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 System and Communications Protection (SC) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text.**

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary.

The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW SC-1	MOD SC-1	HIGH SC-1

SC-2 APPLICATION PARTITIONING

Applicability: Moderate and High Impact Information Systems

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-2	HIGH SC-2

SC-3 SECURITY FUNCTION ISOLATION

Applicability: High Impact Information Systems

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The

information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION IN SHARED RESOURCES

Applicability: Moderate and High Impact Information Systems

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Applicability: All Information Systems

Control: The information system protects against or limits the effects of the following types of denial of service attacks: all flaw-based, SYN flood, ICMP flood, UDP flood, teardrop, application-level flood, nuke and SQL injection attacks.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service

attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	LOW SC-5	MOD SC-5	HIGH SC-5

SC-6 RESOURCE PRIORITY

Applicability: Moderate and High Impact Information Systems

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-6	HIGH SC-6

SC-7 BOUNDARY PROTECTION

Applicability: All Information Systems

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.

Control Enhancements:

1. The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.

   Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

2. The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

3. The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

   Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.

4. The organization:

   a. Implements a managed interface for each external telecommunication service;
   b. Establishes a traffic flow policy for each managed interface;
   c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
   d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
   e. Reviews exceptions to the traffic flow policy at least annually; and
   f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

5. The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
6. The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

7. The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

   Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a

virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent *split-tunneling*. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

8. The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.

   Enhancement Supplemental Guidance: External networks are networks outside the control of the organization. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers are also configurable with organization-defined lists of authorized and unauthorized websites.

12. The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.

    Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.

13. The organization isolates [*Assignment: organization defined key information security tools, mechanisms, and support components*] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.

18. The information system fails securely in the event of an operational failure of a boundary protection device.

    Enhancement Supplemental Guidance: Fail secure is a condition achieved by the application of a set of information system mechanisms to ensure that in the event of an operational failure of a boundary protection device at a managed interface (e.g., router, firewall, guard, application gateway residing on a protected subnetwork commonly referred to as a demilitarized zone), the system does not enter into an unsecure state where intended security properties no longer hold. A failure of a boundary protection device cannot lead to, or cause information external to the boundary protection device to enter the device, nor can a failure permit unauthorized information release.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Priority and Baseline Allocation:

P1	**LOW** SC-7	**MOD** SC-7 (1) (2) (3) (4) (5) (7) **(8) (12) (13) (18)**	**HIGH** SC-7 (1) (2) (3) (4) (5) (6) (7) (8) **(12) (13) (18)**

SC-8 TRANSMISSION INTEGRITY

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

1. The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

   Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-8 (1)	HIGH SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.
Control Enhancements:

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by protective distribution systems.

   Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-113; CNSS Policy 15; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-9 (1)	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Applicability: Moderate and High Impact Information Systems

Control: The information system terminates the network connection associated with a communications session at the end of the session or after thirty minutes of inactivity for all RAS-based sessions; thirty to sixty minutes of inactivity for non-interactive users. Long running batch jobs and other operations are not subject to this time limit.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.

Control Enhancements: None.

References: OMB Memorandums 06-16, 07-16; Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Applicability: Moderate and High Impact Information Systems

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-11	**HIGH** SC-11

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Applicability: All Information Systems

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

Control Enhancements:

1. The organization maintains availability of information in the event of the loss of cryptographic keys by users.
2. The organization produces, controls, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes.
5. The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12 (2) (5)	**HIGH** SC-12 (1) (2) (5)

SC-13 USE OF CRYPTOGRAPHY

Applicability: All Information Systems

Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: None.

Control Enhancements:

1. The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.

References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL, WWW.CNSS.GOV.

Priority and Baseline Allocation:

P1	**LOW** SC-13 (1)	**MOD** SC-13 (1)	**HIGH** SC-13 (1)

SC-14 PUBLIC ACCESS PROTECTIONS

Applicability: All Information Systems

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING DEVICES

Applicability: All Information Systems

Control: The information system:

a. Prohibits remote activation of collaborative computing devices; and
b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-15	**MOD** SC-15	**HIGH** SC-15

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Applicability: Moderate and High Impact Systems
Control: The organization issues public key certificates under an [*Assignment: organization-defined certificate policy*] or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-17	HIGH SC-17

SC-18 MOBILE CODE

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

Control Enhancements:

4. The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and requires [*Assignment: organization-defined actions*] prior to executing the code.

Enhancement Supplemental Guidance: Actions required before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments.

References: NIST Special Publication 800-28; NIST Special Publication 800-28; DOD Instruction 8552.01.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-18	HIGH SC-18 (4)

SC-19 VOICE OVER INTERNET PROTOCOL

Applicability: Moderate and High Impact Systems

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: None.

Control Enhancements: None.

References: NIST Special Publication 800-58.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-19	HIGH SC-19

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUHTORITATIVE SOURCE)

Applicability: All Information Systems

Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

Control Enhancements:

1. The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

   Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	LOW SC-20 (1)	MOD SC-20 (1)	HIGH SC-20 (1)

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Applicability: Moderate and High Impact Information Systems

Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

Control Enhancements: None Mandated.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-21	HIGH SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Applicability: Moderate and High Impact Information Systems

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).

Control Enhancements: None.

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Applicability: Moderate and High Impact Information Systems

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

Control Enhancements: None Mandated.

References: NIST Special Publications 800-52, 800-77, 800-95.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-23	**HIGH** SC-23

SC-24 FAIL IN KNOWN STATE

Applicability: High Impact Information Systems

Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SC-24

SC-25 THIN NODES

Applicability: High Impact Information Systems

Control: The information system employs processing components that have minimal functionality and information storage.

Supplemental Guidance: The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SC-25

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

Applicability: High Impact Information Systems

Control: The information system includes: [*Assignment: organization-defined operating system-independent applications*].

Supplemental Guidance: Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating system are under attack.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD Not Selected	HIGH SC-27

SC-28 PROTECTION OF INFORMATION AT REST

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the confidentiality and integrity of information at rest.

Supplemental Guidance: This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

Control Enhancements:

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.

References: NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD SC-28	HIGH SC-28 (1)

SC-30 VIRTUALIZATION TECHNIQUES

Applicability: Moderate and High Impact Information Systems

Control: The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.

Supplemental Guidance: Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-30	**HIGH** SC-30

SC-32 INFORMATION SYSTEM PARTITIONING

Applicability: Moderate and High Impact Information Systems

Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-32	**HIGH** SC-32

SC-33 TRANSMISSION PREPARATION INTEGRITY

Applicability: High Impact Information Systems

Control: The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

Supplemental Guidance: Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-33

Department of the Interior

Security Control Standard

System and Information Integrity

April 2011

Version: 1.1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	February 4, 2011	Initial draft
Timothy Brown	0.2	February 7, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY 3

TABLE OF CONTENTS 4

SECURITY CONTROL STANDARD: SYSTEM AND INFORMATION INTEGRITY 5

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES 5
SI-2 FLAW REMEDIATION 6
SI-3 MALICIOUS CODE PROTECTION 7
SI-4 INFORMATION SYSTEM MONITORING 8
SI-5 SECURITY ALERTS, ADVISORIES AND DIRECTIVES 9
SI-6 SECURITY FUNCTIONALITY VERIFICATION 10
SI-7 SOFTWARE AND INFORMATION INTEGRITY 10
SI-8 SPAM PROTECTION 11
SI-9 INFORMATION INPUT RESTRICTIONS 12
SI-10 INFORMATION INPUT VALIDATION 12
SI-11 ERROR HANDLING 12
SI-12 INFORMATION OUTPUT HANDLING AND RETENTION 13

SECURITY CONTROL STANDARD: SYSTEM AND INFORMATION INTEGRITY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 System and Information Integrity (SI) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary.

The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW SI-1	MOD SI-1	HIGH SI-1

SI-2 FLAW REMEDIATION

Applicability: All Information Systems

Control: The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
c. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.
Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Control Enhancements:

1. The organization centrally manages the flaw remediation process and installs software updates automatically.

   Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

2. The organization employs automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation.

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	LOW SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Applicability: All Information Systems

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
   - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
   - Inserted through the exploitation of information system vulnerabilities;
b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
   - Perform periodic scans of the information system at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   - Block or quarantine malicious code, send alert to administrator in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Control Enhancements:

1. The organization centrally manages malicious code protection mechanisms.
2. The information system automatically updates malicious code protection mechanisms (including signature definitions).
3. The information system prevents non-privileged users from circumventing malicious code protection capabilities.

References: NIST Special Publication 800-83.

Priority and Baseline Allocation:

P1	**LOW** SI-3	**MOD** SI-3 (1) (2) (3)	**HIGH** SI-3 (1) (2) (3)

SI-4 INFORMATION SYSTEM MONITORING

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Monitors events on the information system to ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise and detect information system attacks;
b. Identifies unauthorized use of the information system;
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP

proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7.

Control Enhancements:

2. The organization employs automated tools to support near real-time analysis of events.
4. The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

   Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

5. The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.

   Enhancement Supplemental Guidance: Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

6. The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-4 (2) (4) (5) (6)	**HIGH** SI-4 (2) (4) (5) (6)

SI-5 SECURITY ALERTS, ADVISORIES AND DIRECTIVES

Applicability: All Information Systems

Control: The organization:

a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities; and
d. Implements security directives in accordance with established timeframes, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is *essential* due to the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

Control Enhancements:

1. The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	**LOW** SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Applicability: Moderate and High Impact Information Systems

Control: The information system verifies the correct operation of security functions upon system startup and/or restart and periodically every ninety days and notifies system administrator when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states include, for example, startup, restart, shutdown, and abort.

Control Enhancements: None Mandated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD SI-6**	**HIGH** SI-6

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Applicability: Moderate and High Impact Information Systems

Control: The information system detects unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

1. The organization reassesses the integrity of software and information by performing monthly integrity scans of the information system.
2. The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-7 (1)	**HIGH** SI-7 (1) (2)

SI-8 SPAM PROTECTION

Applicability: Moderate and High Impact Information Systems

Control: The organization:

a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.

Control Enhancements:

1. The organization centrally manages spam protection mechanisms.

References: NIST Special Publication 800-45.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-8	**HIGH** SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Applicability: Moderate and High Impact Information Systems

Control: The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.

Control Enhancements: None.
References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION INPUT VALIDATION

Applicability: Moderate and High Impact Information Systems

Control: The information system checks the validity of information inputs.

Supplemental Guidance: Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Applicability: Moderate and High Impact Information Systems

Control: The information system:

a. Identifies potentially security-relevant error conditions;

b. Generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g. security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings) in error logs and administrative messages that could be exploited by adversaries; and
c. Reveals error messages only to authorized personnel.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Applicability: All Information Systems

Control: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SI-12	**MOD** SI-12	**HIGH** SI-12

FOUNDATION CLOUD HOSTING SERVICES (FCHS)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY REQUIREMENTS FOR U.S. DEPARTMENT OF THE INTERIOR

FCHS IT SECURITY AND PRIVACY REQUIREMENTS
V1.2

Table of Contents

1. Background 3
2. Applicable Laws, Policy, Rules, Regulations, Standards and Guidelines 4
3. Information Security and Privacy Requirements 9
4. Personnel Security Background Investigations and Clearances 11
5. Non-Disclosure Agreements (NDAs) 12
6. Personnel Changes 12
7. Government access 12
8. Incident Detection, Notification, Handling, Response, Containment, Eradication, Recovery and Reporting 13
9. Federal Information Security Management Act (FISMA) 14
10. Assessment and Authorization (A&A) 15
11. Government support of the FISMA Assessment and Authorization (A&A) Process 16
    11.1 System Security Plan (SSP) 16
    11.2 Continuous Monitoring Plan (CMP) 17
    11.3 Contingency Plan (CP) 19
    11.4 Security Assessment Plan and Report (SAP/SAR) 19
    11.5 Plan of Action and Milestones (POA&M) 20
    11.6 Information Assurance (IA) Requirements 20
        11.6.1 Cloud Service Delivery Model Security Requirements 22
        11.6.2 Independent Verification and Validation (IV&V) 26
        11.6.3 Internet Logon Banner 27
        11.6.4 Logon Warning Banner 27
        11.6.5 Quality Control (Malicious Code) 27
        11.6.6 Security Controls 27
        11.6.7 Training 28
        11.6.8 Privacy 28
12. Roles and Responsibilities 28
13. IT Security Policies, Standards, Guidelines and Other Publications 29
APPENDIX A - IT Security and Privacy Checklist 31
APPENDIX B - Deliverable and Reporting Requirements 32

1. BACKGROUND

The Department of the Interior (DOI) is seeking Foundation Cloud Hosting Services (FCHS) that can meet security control objectives for IaaS, PaaS and SaaS information systems having an overall security categorization of "LOW", "MODERATE" or "HIGH", commensurate with the DOI hosted applications, and corresponding individual potential risk impact ratings of "LOW", "MODERATE" or "HIGH" for the Confidentiality, Integrity and Availability objectives with corresponding management, operational, and technical security controls to adequately protect sensitive agency information, the information system(s) and operating environments employed in the operations and maintenance of the delivery of those services.

As with all Federal government agencies, DOI is subject to numerous requirements stemming from a variety of Laws, rules, regulations, directives, and standards aimed at ensuring the protection of sensitive agency information and information systems. These requirements include providing information security protections commensurate with the risk and magnitude of the potential harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by the agency or by a contractor on behalf of the agency.

Consequently, the Contractor shall also adhere to and comply with applicable Laws, Executive Orders and Executive Branch Policy regarding the design, build, testing, operations and maintenance of the information system and the security controls designed to safeguard agency information. This document establishes the information technology (IT) security and privacy requirements in which the service provider must comply. These requirements are applicable when DOI information is generated, accessed, stored, processed, or exchanged with DOI or on behalf of DOI by a service provider or subcontracted service provider, regardless of whether the information resides on a DOI information system or a service provider/subcontracted service provider's information system. The service provider shall protect the confidentiality, integrity, and availability of DOI electronic information and IT resources and protect DOI electronic information from unauthorized disclosure.

DOI remains responsible and accountable for all risk incurred by use of services provided by external service providers. This risk is addressed by requiring a minimum set of security and privacy controls that must be implemented and monitored to provide assurance that DOI information remains accurate, secure and available. The requirements outlined herein are intended to provide DOI with an acceptable level of trust and controls that must be maintained throughout the lifecycle of the acquisition. This level of trust and controls are maintained by:

1. Reciprocity through a centralized, Federal acquisition vehicle in accordance with the Federal Risk and Authorization Management Program (FedRAMP). In accordance with the OMB memorandum entitled, *Security Authorization of Information Systems in Cloud Computing Environments*, issued on December 8, 2011, the DOI Authorizing Official (AO) anticipates leveraging and accepting provisional authorizations granted by the FedRAMP Joint Authorization Board (JAB), comprised of the Department of Defense (DOD), Department of Homeland Security (DHS) and the General Services Administration (GSA), in granting security authorizations and an accompanying authority

to operate (ATO) for DOI use of the FCHS, to the extent available. DOI does not necessarily anticipate leveraging authorizations granted independently by other individual agencies, but may opt to do so at its discretion;

2. The Provider acquiring the services of an agreed upon independent third-party assessor to test and evaluate the effectiveness of the applicable security controls; and

3. Meeting the IT security and privacy requirements set forth within this document, including satisfying the ongoing requirements identified within the *IT Security and Privacy Checklist (Appendix A)* and eighteen *DOI Security Control Standards* that correspond to the National Institute of Standards and Technology (NIST) Special Publication (SP) 80-53, *Recommended Security Controls for Federal Information Systems,* which identify additional required control enhancements.

2. Applicable Laws, Policy, Rules, Regulations, Standards and Guidelines

At no additional cost to the Government, Offeror shall comply and cause its Provider or subcontractor to agree to comply with all Information Assurance, IT security and privacy laws, regulations, policies and standards that are applicable to Offeror and Provider in their provision of the services to the Government. In addition, Offeror shall agree and Offeror shall cause Provider or subcontractor to agree, to assist the Government in its compliance with the requirements set forth in the Federal Information Security Management Act (FISMA), by successfully completing the Assessment and Authorization (A&A – formerly referred to as Certification and Accreditation (C&A)) required by FISMA, Office of Management and Budget (OMB) policy, and NIST standards for all information systems provided by Offeror and Provider or subcontractor that shall be used in the provision of the Solutions. Offeror shall ensure that Provider or subcontractor shall complete the A&A process on or before providing solutions on-boarding notice. If, during the term of this contract, there are changes to the data protection and privacy laws and regulations, including FISMA, or if there are new US Federal Government requirements applicable to the Government, then the Offeror and the Government will address these changes in a mutually agreed upon Change Management Process.

A number of laws, regulations, directives, policies, standards and guidelines mandate protection of Federal government information, information systems and related resources, including all information systems owned or operated on behalf of the government by the Contractor/Provider. Applicable laws passed by Congress include:

Authority	Description
Federal Records Act of 1950, 44 U.S.C. §§21, 29, 31 and 33	Establishes the framework used by Federal agencies for their Records Management programs.
The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552	This law requires that Federal information be made available to the public except under certain specified conditions.
The Privacy Act of 1974, 5 U.S.C. § 552a	This law imposes collection, maintenance, use, safeguard, and disposal requirements for Executive Branch offices maintaining information on individuals in a "system of records."
Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512	This law mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems.
Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030	This law provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse government resources, and/or conduct fraud on government computers.
Government Performance and Results Act (GPRA) of 1993, 31 U.S.C. § 1101	This law establishes policies for managing agency performance of mission, including performance of its practices.
Paperwork Reduction Act of 1995, Revised, 44 U.S.C. §§ 3501-3520	This law provides for the administration and management of computer resources.
Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 1401 et seq.	This law improves the acquisition, use, and disposal of Information Technology (IT) by the Federal government.
Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111	This law mandates Federal agencies to implement and maintain financial management systems that comply substantially with Federal systems requirements, Federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act.
National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030	This law provides for the protection of computer resources.
Government Paperwork Elimination Act (GPEA) of 1998, 44 U.S.C. § 3504	This law provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content.

Authority	Description
E-Government Act of 2002, 44 U.S.C. § 101	This law enhances the management and promotion of electronic government services and processes by establishing a broad framework of measures requiring technology to enhance citizen access to government information services.
Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541	FISMA requires Federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.

The following are Executive Orders that provide details related to information security for Federal Agencies.

Executive Order 10450, Security Requirements for Government Employees, April 1953	This order establishes that the interests of national security require all government employees be trustworthy, of good character, and loyal to the United States.
Executive Order 13011, Federal Information Technology, July 1996	This order establishes policy for the head of each agency to effectively use information technology to improve mission performance and service to the public.
Executive Order 13103, Computer Software Piracy, September 1998	This order establishes policy that each executive agency shall work diligently to prevent and combat software piracy in order to give effect to copyrights associated with computer software.
Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998	This directive requires that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures, including our cyber systems.
Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001	This order establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems.

The following are Executive branch policies established through directives published by OMB based on the applicable laws passed by Congress.

OMB Circular	Description
A-11, Section 53, Information Technology and E-Government	This directive specifies the identification of security and privacy safeguards for managing sensitive information.
A-123, Management Accountability and Control, as revised December 21, 2004	This directive specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies.
A-127, Financial Management	This directive prescribes policies and standards for

OMB Circular	Description
Systems, as revised by Transmittal Memorandum Number 3, December 1, 2004	executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.
A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals	This directive prescribes policy to agencies for the implementation of the Privacy Act and reporting requirements related to the management of personally identifiable information (PII).
A-130, Appendix III, Security of Federal Automated Information Resources, as revised by Transmittal Memorandum Number 4, November 28, 2000	This directive stipulates that each agency shall implement a comprehensive automated information security program. The appendix establishes basic managerial and procedural controls that shall be included in Federal automated information systems.

The Contractor shall also ensure conformance and compliance with, and provide services that implement and meet, the following requirements:

- OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.*

- OMB Memoranda M-06-16, *Protection of Sensitive Agency Information*, and M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which establish requirements for the use of two-factor authentication for remote system access and requirements for responding to breaches or possible breaches of Personally Identifiable Information (PII).

- OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections*, which establishes the requirement for DOI to comply with the Trusted Internet Connection (TIC) initiative and the architectural requirements defined by the Department of Homeland Security (DHS) in the TIC Reference Architecture (current version 2.0 dated 2011).

- OMB Memorandum M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form.*

- Office of Management and Budget (OMB) Memorandum M-08-26, *Transition from FTS 2001 to Networx.*

- OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection Compliance.*

- OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors.*

- OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

- National Security Presidential Directive and Homeland Security Presidential Directive (NSPD-54/HSPD-23), *Comprehensive National Cyber Security Initiative.*

- Homeland Security Presidential Directive (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors.*

- Department of Homeland Security (DHS) Trusted Internet Connection (TIC), Version 2.0, Reference Architecture requirements.

- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance and associated NIST standards regarding implementation and use of HSPD-12 Personal Identity Verification (PIV) two-factor SmartCard Public Key Infrastructure (PKI) based credentials for logical authentication.

- NIST Federal Information Processing Standard (FIPS) Publications.

- NIST 800-series Special Publications (SP).

- NIST Security Technical Implementation Guides (STIGs – also referred to as security configuration checklists).

- All management, operational and technical security control and continuous monitoring requirements as specified by FedRAMP.

- DOI TIC security architecture.

- DOI IT security and privacy policies, standards, guidelines and procedures to include, but not limited to, the following:

  - DOI Departmental Manual (DM) 375DM19;

  - DOI Security Control Standards (i.e., the eighteen (18) DOI-specific security control family standards based on the NIST SP 800-53 security control families that include agency-wide standard parameters, values, etc. for certain controls and that incorporate additional controls or control requirements for implementations within cloud computing environments; and

  - DOI-specific standards, procedures and security requirements specified in the following:

    - DOI Plan of Actions and Milestones (POA&M) Process Standard;

- ❖ DOI Computer Security Incident Response Handbook and associated incident notification, response, handling and reporting requirements;

- ❖ Privacy Loss Mitigation Strategy (PLMS) and associated Breach Incident Reporting and Handling Procedures; and

3. INFORMATION SECURITY AND PRIVACY REQUIREMENTS

Service providers are required to comply with the security and privacy requirements summarized in this section and identified in the *IT Security and Privacy Checklist (Appendix A)*, NIST standards and the *DOI Security Control Standards* established using the NIST SP 800-53. All applicable security and privacy controls identified herein, and in the *DOI Security Control Standards,* shall be assessed in accordance with the NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations.*

The level of compliance with the required minimum baseline security and privacy controls are determined by DOI to ensure a level of trust with the service provider and that the risk from using external services is at an acceptable level to the DOI authorizing official.

- **Security and Privacy Requirements.** DOI requires that the service provider implement the security controls identified herein, in the *IT Security and Privacy Checklist (Appendix A)* and in the *DOI Security Control Standards,* to ensure the confidentiality, integrity, and availability of DOI information. A summary of some of the key security requirements is as follows:

    - o Under some circumstances, the use of public or hybrid clouds and their associated risks may be deemed acceptable by the DOI Authorizing Official (AO) who shall make the risk-based determination in consultation with, and with the concurrence of, the Department's Chief Information Officer (CIO). DOI is not aware of public or hybrid cloud solutions at this time that would meet the security requirements defined in this solicitation, federal policy, and individual task orders for "MODERATE" systems, but may become aware of these through the solicitation process or otherwise in the future. DOI does not wish to preclude potential interagency customers from implementing hosting in public or hybrid cloud solutions based upon their independent risk management processes, or to preclude hosting of moderate systems in public or hybrid clouds if, and when, the specific security requirements defined in the RFP and the individual Task Orders can be met.

    - o All service provider information system components that access, store, transmit and/or process DOI information must be located within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and/or the Virgin Islands);

- Trusted Internet Connection 2.0 - The IaaS, PaaS and SaaS must provide a Trusted Internet Connection 2.0 (TIC 2.0, see http://www.dhs.gov/files/programs/gc_1268754123028.shtm) compliant interconnection architecture.

- IPv6 - The IaaS, PaaS and SaaS must comply with federally mandated IPv6 requirements (see http://www.cio.gov/documents/IPv6memofinal.pdf).

- Identity, Authorization and Access Management (IdAAM) - The IaaS, PaaS and SaaS must seamlessly integrate with the DOI IdAAM solution that consists of the Microsoft Active Directory (AD) and Public Key Infrastructure (PKI) architecture and associated Certificate Authority and DOI HSPD-12 PIV SmartCard-based credentials and enable logical authentication utilizing those credentials without requiring additional Contractor solution credentials. DOI uses Microsoft's Active Directory to create a single DOI-Wide directory of all users. This directory is known as the Enterprise Active Directory (EAD). The FCHS IaaS, PaaS and SaaS must recognize the EAD as the authoritative source for authentication. DOI currently utilizes name and password authentication, however the Department is transitioning to Entrust PKI for authentication. The IaaS, PaaS and SaaS shall support authentication using DOI's Entrust PKI. It is envisioned that in the future all users will authenticate with the Entrust PKI and use the HSPD-12 PIV Smart Card; for the present some users will continue to be authenticated by user name and password, and this method must also be supported.

- DOI must be granted access to service provider facilities in legal, chain of custody scenarios that may arise and upon request to ensure that an acceptable level of trust is maintained;

- All service provider personnel must undergo background investigation, performed by the Office of Personnel Management, prior to being granted logical or physical access to DOI information; and

- The service provider will share all DOI information with DOI using an agreed upon secure transmission method to ensure the security of DOI information.

- **Security Assurance Requirements.** DOI requires that the service provider develop a Security Assessment Plan and initially assess all applicable security controls, using an agreed upon independent third-party assessor, and provide security assessment results in a Security Assessment Report for all applicable security controls (identified herein, in the *IT Security and Privacy Checklist (Appendix A)* and in the *DOI Security Control Standards)*, including an appropriate characterization and articulation of known remaining risks, to support the DOI AO's authorization to operate (ATO).

- **Continuous Monitoring Requirements.** DOI requires that the service provider comply with the continuous monitoring requirements consistent with applicable NIST standards. The service provider is required to share information in accordance with the continuous monitoring requirements defined for the applicable security controls. A Continuous Monitoring Plan (CMP) shall be developed by the service provider that focuses on specific requirements for monitoring the ongoing effectiveness of all applicable security controls (identified herein, in the *IT Security and Privacy Checklist (Appendix A)* and in the *DOI Security Control Standards)*, monitoring frequencies, and security status reporting frequencies and formats to the DOI Authorizing Official (AO), including all associated measures and metrics. (*DOI Security Control Standards* and in accordance with NIST SP 800-53A and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*).

4. PERSONNEL SECURITY BACKGROUND INVESTIGATIONS AND CLEARANCES

Acquired services shall comply with the following regulations and requirements. Homeland Security Presidential Directive-12 requires that all federal entities ensure that all contractors have current and approved security background investigations that are equivalent to investigations performed on federal employees. The Contractor shall comply with DOI policy relating to HSPD-12. Background investigations will be performed by the Office of Personnel Management (OPM) (See DIAPR 2010-04, Implementation of Homeland Security Presidential Directive-12 (HSPD-12) Part 2, DOI Access Program Implementation at http://www.doi.gov/pam/DIAPR%202010-04.pdf).
DOI separates the risk levels for personnel working on federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk. The level/complexity of background investigations must be the same as for a Federal employee holding a similar position. Criteria for determining which risk level a particular contract employee falls into are shown in Illustration 1 of DOI's Departmental Manual (DM) 441, Chapter 3 (available at: http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3860). The DM Chapter provides guidance for the appropriate background investigations based on types of access. The Contractor shall ensure that only appropriately cleared personnel are assigned to positions that meet these criteria.

Those contract personnel determined to be in a:

- Low Risk position will require a National Agency Check with Written Inquiries (NACI) or equivalent investigation;

- Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination; and

- High Risk position will require a Background Investigation (BI).

The Contracting Officer, through the Contracting Officer's Technical Representative or Program Manager will ensure that a completed Contractor Information Worksheet (CIW) for each Applicant is forwarded to the Federal Protective Service (FPS) in accordance with the DOI//FPS Contractor Suitability and Adjudication Program Implementation Plan dated 20 February 2007. FPS will then contact each Applicant with instructions for completing required forms and releases for the particular type of personnel investigation requested.

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or DOI, there has been no break in service, and the position is identified at the same or lower risk level. After the required background investigations have been initiated, the Contractor may request authorization for employees whose investigations are pending to access systems supporting DOI FCHS applications. The DOI Chief Information Officer may grant this authorization based on determination of risk to the government and operational need for the support of these applications.

Contractor shall comply and cause Provider to agree to comply with the United States Government and the DOI regulations as outlined in DM441, Chapter 3, in reference to background checks, position risk and sensitivity. The Provider is responsible for maintaining an up to date list of all personnel that have access to DOI data. This list shall be provided by the service provider at any time during the life of the contract when requested by the CO or COR via email. The vendor shall provide the list within three business days of the request.

5. NON-DISCLOSURE AGREEMENTS (NDAS)

The Offeror shall require each employee that interfaces with the DOI cloud services data, its management, hosting, and delivery to sign non-disclosure agreements prior to beginning work on the DOI contract. Standard non-disclosure statements shall be provided as required for system administration personnel who may have access to government data in the course of their duties. NDAs typically utilized by the Offerer/Provider required to be signed by contractor staff may be utilized in lieu of the DOI standard NDAs provided they are deemed appropriate and acceptable by the Contracting Officer.

6. PERSONNEL CHANGES

The Provider shall notify the COR immediately when key employees having access to the FCHS system or DOI information are reassigned or leave the contractor's employ, and prior to an unfriendly termination.

7. GOVERNMENT ACCESS

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, availability, and reliability of any non-public government data collected and stored by the Offeror, the Offeror shall afford the government

access to the Offeror's facilities, installations, technical capabilities, operations, documentation, records and databases. The Provider shall also identify how the following compliance, oversight and law enforcement objectives can be effectively and efficiently conducted by DOI in the event such activity is deemed by DOI to be appropriate and necessary relative to the facilities, installations, operations, documentation, databases, IT systems, devices, and personnel used in performance of the contract, regardless of the location:

- audits;
- inspections;
- evaluations;
- investigations;
- continuous monitoring of the security posture and continued effectiveness of management, operational and technical controls (including IT asset and device discovery, inventory and security configurations);
- penetration testing; and
- vulnerability testing.

The above are in addition to the similar types of activities outlined herein that are normally conducted by the Provider or independent assessors. Such activities are expected to occur only in rare instances where DOI determines that special circumstances necessitate additional measures to ensure the FCHS system is employing adequate safeguards against specific threats and hazards to the confidentiality, integrity and availability of DOI data/information or to the function of the FCHS system and the preservation of evidence of computer crimes.

The above objectives may be achieved by employing the services of mutually agreed to independent third-party auditors, inspectors, evaluators, investigators, or assessors as deemed appropriate by DOI. All associated information shall be available to DOI upon request.

8. INCIDENT DETECTION, NOTIFICATION, HANDLING, RESPONSE, CONTAINMENT, ERADICATION, RECOVERY AND REPORTING

The Provider shall immediately report all incidents, whether suspected or confirmed, involving potential risks to the confidentiality, integrity or availability of DOI's information or to the function of FCHS systems operated on behalf of DOI, to the DOI Computer Incident Response Center (DOI-CIRC), DOI Contracting Officer and DOI System Owner. The Provider shall report computer security incidents and breaches affecting DOI data/information or to the function of FCHS systems in accordance with the DOI Computer Incident Response Handbook. The Provider shall promptly coordinate with the DOI System Owner and DOI-CIRC on all related FCHS incident handling, response, containment, eradication, and recovery efforts throughout the incident lifecycle until fully resolved to the satisfaction of the DOI System Owner.

Upon becoming aware of any unlawful access to any DOI data/information stored on Provider's equipment or in Provider's facilities, or unauthorized access to such facilities or equipment resulting in loss, disclosure or alteration of any DOI data/information (a "Security Incident"), Provider will:

(i) immediately notify the CO and COR's via email with details of the Security Incident;
(ii) investigate the Security Incident and provide DOI with detailed information about the Security Incident; and
(iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

If new or unanticipated threats or hazards are discovered by either the government or the Offeror, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

9. FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)
At all times, the Contractor shall comply and the Contractor shall cause Provider to agree to comply with FISMA and OMB Circular A-130. This compliance shall include the completion and ongoing maintenance of the Assessment and Authorization (A&A – formerly referred to as Certification and Accreditation (C&A)) of the Provider service and adherence to DOI Policies on IT Security Management. The maintenance of the A&A is a requirement of the business relationship between DOI, the Contractor and Provider.

Continued utilization of the service by any DOI entity shall be dependent upon the completion and maintenance of the A&A.

The following NIST Federal Information Processing Standard Publications (FIPS Pubs) and Special Publications (SPs) are especially applicable to the Product Acquisition. They are A&A focused. Successful completion of A&A includes, but is not limited to, these standards:

NIST Standards
FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*
FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*
SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
SP 800-34, *Contingency Planning Guide for Federal Information Systems*
SP 800-30, *Guide for Conducting Risk Assessments*
SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*

Figure 1 – NIST A&A Related Standards

10. ASSESSMENT AND AUTHORIZATION (A&A)

The Offeror, using an independent assessor approved by the DOI Authorizing Official (AO), will perform the Assessment and Authorization (A&A – formerly referred to as Certification and Accreditation (C&A)) of the FCHS information system developed or maintained hereunder prior to going into production. Subsequent to the initial authorization to operate, required to be formally approved by the DOI AO, DOI requires that the FCHS information system follow the ongoing authorization process and associated continuous monitoring requirements as prescribed by OMB and NIST. This Provider shall assess the effectiveness of required implemented controls on an ongoing basis to inform the AO's decisions regarding the continued use and operation of the system. A&A documents will be provided to the COR, DOI System Owner, and DOI AO in both hard copy and electronic forms.

The Contractor must obtain the appropriate A&A through validation of *security functionality* of required management, operational, and technical controls selected, documented in the System Security Plan (SSP), and formally approved by the DOI AO. The security control objectives for the FCHS IaaS, PaaS and SaaS information systems shall meet the overall security categorizations of "LOW", "MODERATE" or "HIGH" commensurate with the DOI hosted applications, and corresponding individual potential risk impact ratings of "LOW", "MODERATE" or "HIGH" for the Confidentiality, Integrity and Availability objectives and shall have selected and implemented appropriate security controls corresponding to those security categorizations (see NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*). Security functionality must be obtained by employing within the information system and its environment of operation, a combination of the appropriate set of management, operational, and technical security controls from NIST Special Publication 800-53 that correspond to the security categorization and associated potential risk impact ratings.

The Contractor must follow all relevant NIST FIPS Pubs and SPs to include, but not limited to, FIPS Pub 199 and 200, SP 800-39, 800-37, 800-137, 800-60, 800-53, 800-53A, 800-34, 800-30, and 800-18. The Contractor must also comply with all DOI IT security and Privacy policies and standards including, but not limited to, Departmental Manual (375DM19); DOI Security Control Standards (SCS), including the eighteen security control family standards; and the DOI Privacy Impact Assessment (PIA) requirements and associated templates.

Where the security control requirements outlined herein cannot be met, at the discretion of and approval by the DOI AO, either:

- other alternative mitigating/compensating controls can be offered by the Contractor for consideration and approval by the DOI AO;
- the DOI AO can formally document and accept the associated risk of not implementing a control or the residual risk level resulting from partial risk mitigation; or
- the DOI AO can reject risk acceptance and the proposed solution by not authorizing the system to operate.

Where a proposed FCHS information system provides for sufficient physical separation as a compensating/mitigating control obviating the need to impose one or more requirements outlined herein, the Contractor should provide the appropriate rationale and justification supporting such assertions for consideration, risk acceptance, and approval by the DOI AO.

The DOI AO for the FCHS information system is the Department's Chief Information Officer (CIO).

The A&A on DOI systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

11. GOVERNMENT SUPPORT OF THE FISMA ASSESSMENT AND AUTHORIZATION (A&A) PROCESS

The Government will timely review Provider's Assessment and Authorization (A&A) documentation package and any changes submitted by Provider that could require re-assessment in order to assist the Government in its compliance with FISMA and the NIST 800-53 security control requirements. If there are any errors, omissions or other issues with the Provider's A&A documentation package or assessment results, the Government will timely notify Provider and provide reasonable descriptions of specific errors, omission or other issues. The Government will reasonably cooperate with Provider in the A&A process and will not unreasonably withhold or delay any review of A&A package documentation, assessment result from the independent assessor, or authorization decisions.

Upon completion and acceptance of the A&A the Contractor is responsible for providing all signed documentation to the Contracting Officer and COR's.

11.1 SYSTEM SECURITY PLAN (SSP)

As part of the A&A, the Contractor shall develop a SSP in conformance with NIST SP 800-37, 800-39, 800-18, 800-60, 800-53, 800-137 and FIPS Pubs 199 and 200.

In addition to the NIST SP 800-53 minimum security control requirements applicable to the FCHS IaaS, PaaS and SaaS information system components having appropriate security controls selected and implemented for security categorizations of "LOW", "MODERATE" or "HIGH" commensurate with the DOI hosted applications, the following additional requirements and enhancements apply:

11.1.1 Auditable Events (AU-2) Control

In addition to the types of events to be audited as specified by FedRAMP, the FCHS shall include automated auditing, alerting and reporting of all events in which any individual, other than the intended authorized individual(s), accesses any DOI information. Such events shall constitute a potential security violation, unless such access has been explicitly and formally approved by the DOI System Owner in writing, and reported to DOI as a potential incident in accordance with section 8 above (see *Incident Detection, Notification, Handling, Response, Containment, Eradication, Recovery and Reporting*).

11.1.2 Maintenance Personnel (MA-5) Control

Control Enhancements

1. The organization maintains procedures for the use of maintenance personnel that lack appropriate background investigations and security clearances or are not U.S. citizens, that include the following requirements:

    a. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

    b. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

    c. In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.

    Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any Controlled Unclassified Information (CUI); information subject to the Privacy Act, including Personally Identifiable Information (PII); or any other sensitive agency information contained on the information system. Procedures for the use of maintenance personnel shall be documented in the security plan for the information system.

2. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are cleared (i.e., possess appropriate background investigations and security clearances) for the highest level of information on the system.

3. The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting sensitive agency information are U.S. citizens.

11.2 Continuous Monitoring Plan (CMP)

The Provider shall submit a continuous monitoring plan that supports the DOI AO's ongoing authorization process. The plan must conform to the NIST SP 800-137 and be formally approved by the DOI AO. The Contractor shall submit monthly continuous monitoring reports to the applicable Government System Owner and Authorizing Official.

The Contractor is required to conduct continuous monitoring of the FCHS information system in a manner that enables enterprise-wide visibility into the security posture and effectiveness of controls across the FCHS. The Contractor is required to monitor the security state of the FCHS information system on an ongoing basis with a frequency sufficient to enable the DOI AO to make ongoing risk-based decisions on whether to continue to utilize the system. The Contractor

shall develop, document, and implement a continuous monitoring program for the FCHS information system and obtain approval of the continuous monitoring strategy by the DOI AO.

The continuous monitoring program must address, at a minimum: (i) the effectiveness of deployed security controls; (ii) changes to information systems and the environments in which the system operates; and (iii) compliance to federal legislation, directives, policies, standards, and guidance with regard to information security and risk management. In documenting the continuous monitoring program for the FCHS information system, the Contractor must identify and obtain approval by the DOI AO for the security controls to be monitored, the frequency of monitoring, and the control assessment approach. The program must define how changes to the FCHS information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements including recipients of the status reports.

The Contractor must apply the guidance provided in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and the supporting NIST SP 800-137, *Information System Continuous Monitoring for Federal Information Systems and Organizations*, in developing and implementing their continuous monitoring strategy for the FCHS information system. The Contractor shall take into consideration the criteria provided in the NIST standards in determining control assessment and monitoring frequencies. These criteria, as well as those provided in applicable OMB guidance for FISMA reporting (including associated Department of Homeland Security requirements for reporting of key metrics through submission of required data feed elements into CyberScope from automated security management tools), shall be used in determining the methodology for continuous monitoring supporting the ongoing system authorization process.

Information systems used or operated by Federal agencies, or by contractor(s) on their behalf, must be tested and evaluated annually. The security control assessment results may be drawn upon from the following sources to satisfy the annual FISMA requirement, including but not limited to:

- Security assessments conducted as part of an information system security authorization or re-authorization process;
- Continuous monitoring activities; or
- Testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that testing and evaluation results are current and relevant to the determination of security control effectiveness).

Automated monthly discovery and reporting of all associated FCHS system physical and logical assets shall be conducted to maintain an accurate physical and logical inventory of all system components. Automated monthly vulnerability scans and verification of security configurations for all FCHS system physical and logical assets shall be conducted using authenticated and agent-based mechanisms to ensure the most comprehensive and accurate detection, identification and reporting of vulnerabilities and weaknesses in the FCHS information system and associated components. An electronic copy of each report and session data shall be provided to the COR and System Owner.

At least annually, the FCHS information system and associated components accessible from the Internet must be penetration tested by a mutually agreed to independent third-party assessor. Electronic and hard copy reports of penetration test results shall be provided to the COR and System Owner.

The Government reserves the right to conduct prearranged vulnerability scans or penetration tests using a mutually agreed to independent third-party assessor in accordance with a formally documented Memorandum of Agreement (MOA) and accompanying Rules of Engagement.

The Provider will take appropriate and timely action to correct or mitigate weaknesses discovered during such testing, at no additional cost.

The Contractor's continuous monitoring program shall include providing, implementing, and maintaining all Security Content Automation Protocol (SCAP[1]) compliant data feeds for all of the types of data elements (e.g., asset inventory and security configuration) required by the Department of Homeland Security (DHS) and upload them to the DHS CyberScope[2] solution within the frequencies and formats established by DHS.

11.3 Contingency Plan (CP)

The Provider shall submit a contingency plan for restoration and testing of FCHS system services and resumption of maintenance support during a contingency operation. The plan must conform to the NIST SP 800-34 and be consistent with existing DOI continuity of operation procedures and plans. The Contractor shall submit contingency plans to the DOI System Owner.

11.4 Security Assessment Plan and Report (SAP/SAR)

The Offeror, using an independent third-party assessor approved by the DOI AO, will plan and conduct the security assessment of the FCHS information system in accordance with NIST SP 800-53A and document all identified vulnerabilities and weaknesses and appropriately characterize and assess the resulting risks in accordance with NIST SP 800-30 in the SAR.

The qualifications and required degree of independence of the assessors shall be at the discretion and approval of the DOI AO.

With the approval of the Government System Owner, and as required by the DOI AO, the Contractor will take immediate and timely action to correct or mitigate any vulnerabilities and weaknesses discovered, as necessary, to bring the application or system into compliance with the IT security and Privacy requirements outlined herein.

[1] See http://scap.nist.gov/

[2] See http://scap.nist.gov/use-case/cyberscope/

11.5 Plan of Action and Milestones (POA&M)

The Provider shall develop and maintain a POA&M documenting all known IT security vulnerabilities and weaknesses in the FCHS information system and associated components. The POA&M must contain the required elements identified in the DOI POA&M Processing Standard. The Contractor shall submit POA&Ms to the DOI System Owner and, in coordination with the DOI System Owner, provide quarterly briefings to the DOI AO regarding the corrective action status of known vulnerabilities and weaknesses and the risks they pose to DOI's information and the FCHS information system.

11.6 Information Assurance (IA) Requirements

The Contractor services and associated solutions shall also implement the following requirements:

- Encryption of all sensitive data in transit (motion) and at rest (storage) using only NIST Validated FIPS 140-2 compliant and validated cryptographic modules and algorithms.

- Under some circumstances, the use of public or hybrid clouds and their associated risks may be deemed acceptable by the DOI Authorizing Official (AO) who shall make the risk-based determination in consultation with, and with the concurrence of, the Department's Chief Information Officer (CIO). DOI is not aware of public or hybrid cloud solutions at this time that would meet the security requirements defined in this solicitation, federal policy, and individual task orders for "MODERATE" systems, but may become aware of these through the solicitation process or otherwise in the future. DOI does not wish to preclude potential interagency customers from implementing hosting in public or hybrid cloud solutions based upon their independent risk management processes, or to preclude hosting of DOI moderate systems in public or hybrid clouds if, and when, the specific security requirements defined in the RFP and the individual Task Orders can be met

- Access, transmit, process, house, and store all sensitive agency information, including information subject to the Privacy Act and Personally Identifiable Information (PII), only within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands).

- Conduct annual penetration testing using a qualified and competent independent third-party assessor/evaluator subject to approval by the DOI AO.

- Implement cloud service infrastructure and data storage redundancy in at least two facilities located within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands) with adequate geographical separation of at least 250 miles with one serving as the primary site and the other as an alternate backup Disaster Recovery (DR) site capable of restoration and resumption of FCHS services and complete preservation

and reconstitution of all DOI data/information within 24 hours of failure of the services normally provided by the primary site.

- Seamlessly integrate with the DOI Identity, Authorization and Access Management (IdAAM) solution that consists of the Microsoft Active Directory (AD) and Public Key Infrastructure (PKI) architecture and associated Certificate Authority and DOI HSPD-12 PIV SmartCard-based credentials and enable logical authentication utilizing those credentials without requiring additional Contractor solution credentials; digital and electronic signing and signatures of emails and documents/content within the collaboration suite; and encryption of emails and documents/content using those capabilities.

- Provide a Data Loss Prevention (DLP) capability for the FCHS to detect and prevent the potential loss, exposure, or confidentiality risks to DOI's sensitive agency information, including information subject to the Privacy Act and Personally Identifiable Information (PII), resulting from intentional or unintentional disclosure to external entities.

- The DLP capability shall be integrated in a manner that allows the agency to specify which recipient domains or individual entities are allowed (e.g., .GOV domains) to receive/access certain types of sensitive agency information (e.g., DOI business partners, and other external organizations whose security environments have been appropriately vetted and authorized to handle such information in a secure manner) and where such sensitive information is detected and domains or individual entities are approved that the content is encrypted by the application residing within the FCHS.

- Provide E-Discovery capabilities that enable compliance with legal mandates and requests capabilities to support legal hold requests.

- Provide solutions that conform to the Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) security configuration requirements; and that are compatible with end-user client computing devices, operating systems, and client software/interfaces (e.g., workstations, laptops, mobile/portable devices) that are configured in accordance with those specifications; and that do not alter, or require alteration of, those baseline standard security configurations.

- Conform to, and implement the requirements of, the *Domain Name System (DNS) Security Reference Architecture*, Version 1.0 or later.

11.6.1 CLOUD SERVICE DELIVERY MODEL SECURITY REQUIREMENTS

The following General Requirements apply to all cloud service delivery models:

(1) **Data Protection.** Obtain appropriate security assurance (see NIST SP 800-39) through an independent third-party assessor's analysis of the provider's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the agency.

(2) **Multi-tenancy.** Under some circumstances, the use of public or hybrid clouds and their associated risks may be deemed acceptable by the DOI Authorizing Official (AO) who shall make the risk-based determination in consultation with, and with the concurrence of, the Department's Chief Information Officer (CIO). DOI is not aware of public or hybrid cloud solutions at this time that would meet the DOI security requirements for "MODERATE" systems, but may become aware of these through the solicitation process or otherwise in the future. DOI does not wish to preclude potential interagency customers from implementing hosting in public or hybrid cloud solutions based upon their independent risk management processes, or to preclude hosting of DOI moderate systems in public or hybrid clouds if, and when, the specific security requirements defined in the RFP and the individual Task Orders can be met.

(3) **Operating Policies.** Contractor shall:

a. submit to and fully cooperate with external audits, evaluations, assessments and security certifications to include, but not limited to, DOI approved and authorized IT security and Independent Verification and Validation (IV&V) staff employees or their designated support contractors, DOI Office of Inspector General (OIG), and the General Accountability Office (GAO);

b. establish incident response and recovery procedures and practices that integrate DOI Computer Incident Response Center (DOI-CIRC) and DOI Advanced Security Operations Center (ASOC) incident and breach detection, reporting, notification, handling, response, containment, eradication and recovery processes and that adequately inform DOI senior agency officials, AO, System Owner, and Information System Security Officer (ISSO) of incidents, remediation and containment actions, etc.

c. submit to and fully cooperate with internal investigation processes with respect to illegal or inappropriate usage of IT resources including, but not limited to, those investigations conducted by the Department's Office of Human Resources for administrative investigations and those conducted by the OIG Computer Crimes Investigation Unit;

d. identify policies and procedures for vetting of privileged uses such as the provider's system and network administrators that are deemed appropriate and acceptable to the DOI AO.

(4) **Authentication.** Contractor shall support the enablement and use of strong authentication tokens in accordance with the Federal Identity, Credential, and Access Management (FICAM) implementation guidance, Homeland Security Presidential Directive (HSPD-12), and associated NIST standards and publications regarding use of the Personal Identity Verification (PIV) Smartcard logical authentication credentials for access to the cloud environment, software, applications, services or infrastructure by either provider or subscriber authorized system administrators and subscriber end-users in a manner that leverages DOI's existing authentication infrastructure to mitigate the risk of account compromise or hijacking.

(5) **Application Configuration.** Applications (including all associated IaaS, PaaS, and SaaS components shall be configured, as necessary, to run in a secure manner (e.g., a dedicated VLAN segment) and shall be integrated with existing enterprise/agency security frameworks (such as Identity, Authorization and Access Management (IdAAM) solution(s), Trusted Internet Connection (TIC) security infrastructure protection architecture, and Trusted Internet Connection Access Provider (TICAP) processes and procedures) such that enterprise/agency security policies are enforced through automated monitoring and detection. This includes ensuring, where necessary, all required components to route applicable and necessary application/network communications traffic through the DOI Trusted Internet Connection (TIC) gateways for monitoring and inspection consistent with DOI's Trusted Internet Connection Access Provider (TICAP) and associated Advanced Security Operations Center (ASOC) security monitoring requirements, including any associated and/or required infrastructure security architecture protection systems, tools, and technologies in conformance with Office of Management and Budget (OMB) and Department of Homeland Security (DHS) TIC requirements and required capabilities.

(6) **Secure Data Deletion and Disposition.** Contractor shall provide a mechanism for reliably deleting DOI data upon request by DOI as well as providing evidence that the data was deleted.

(7) **Data Recovery.** The Contractor shall submit to, and fully cooperate with, DOI personnel to examine the capabilities of the provider with respect to:

a. data backup;
b. data archiving; and
c. data recovery.

(8) **Physical.** The Contractor shall document and demonstrate adequate physical plant security practices and plans at provider sites that are deemed appropriate and acceptable to the DOI AO. Backup plans resulting from both physical and cyber attacks shall be incorporated into the overall plans. The Contractor shall offer redundancy for the sites they operate and provide sufficient geographic separation between alternate disaster recovery locations continued and/or reconstituted within mutually agreed upon timeframes established through Service Level Agreements (SLAs) in case of natural disasters or other disruptions.

(9) **Acceptable Use Policies.** The Contractor shall not impose on DOI employees or contractors any additional requirements other than those articulated in DOI policies (e.g., IT Security, Privacy, Human Resources acceptable use policy, etc.) nor impose any penalties or sanctions on, or against, DOI employees for resolution of policy violations and accept that DOI's handbook on Charges and Penalty Selection for Disciplinary and Adverse Actions, and associated Table of Penalties, are acceptable and to be applied at the management discretion of the agency.

(10) **Licensing.** The Contractor shall properly license any proprietary software installed into their environment where DOI has a dependency on such software and associated functionality delivered by the provider as part of its service.

(11) **Patch Management.** The Contractor shall document a set of procedures for DOI approval and agreement for what DOI needs to perform to take an application offline (whether a software patch is going to be installed by the provider or subscriber), the testing that must be performed to ensure the application continues to perform as intended, and the procedures needed to bring the application back online. Plans for system maintenance should be expressed in a Service Level Agreement (SLA).

(12) **Legal.** Contractor shall offer capabilities to support ad hoc legal requests for:
   a. e-Discovery, such as litigation freezes, and
   b. preservation orders of data and meta-data.

For Software as a Service (SaaS) components, the Contractor shall demonstrate the following to the satisfaction and approval of the DOI AO.

(1) **Client Device/Application Protection.** Consistent with the FIPS 199 security categorization and potential risk impact level of the data being processed (e.g., "LOW", "MODERATE" or "HIGH" for each of DOI's specific requirements commensurate with the security categorizations of DOI's hosted applications), demonstrate to the independent third-party assessor that the cloud subscriber's client devices (e.g., the agency's client computers and mobile devices and associated client software that are necessary to interface with the FCHS) are

adequately protected so as to control the exposure of the agency's network and associated network resources and those of the FCHS to attacks.

(2) **Encryption.** Strong encryption is required to be enforced by the SaaS application using a robust algorithm with keys of required strength in accordance with NIST FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*, and NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, to be used for client sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. For Web sessions the Transport Layer Security Version 1.0 (TLS 1.0) protocol using the Advanced Encryption Standard (AES) 256 bit key cipher suite shall be enforced. The same diligence shall be applied to stored data using the AES 256 bit key cipher suite. All cryptographic algorithms and modules employed shall be only those approved for use by the Federal government and that have been tested, validated and approved by NIST through the Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) and operating in a configuration mode that maintains the integrity of those protective measures.

For Infrastructure as a Service (IaaS) components, the Contractor shall demonstrate the following to the satisfaction and approval of the Authorizing Official (AO).

(1) **Multi-tenancy.** When an IaaS cloud provider provides computing resources in the form of Virtual Machines (VMs), the provider shall have mechanisms in place to protect VMs from attacks

a. from other VMs on the same physical host;
b. from the physical host; as well as
c. network originated attacks.

Typical attack detection and prevention mechanisms shall include Virtual Firewalls, Virtual IDS/IPS etc and network segmentation techniques such as VLANs.

(2) **Administrative Access.** The IaaS cloud provider shall ensure that a limited set of DOI approved and authorized trained/trusted users (from the agency) alone are provided administrative access to any and all rented computing resources in the form of virtual machines or physical servers.

(3) **VM Migration.** A documented strategy for future migration of Virtual Machines and their associated storage among alternate cloud providers shall be developed and maintained by the Contractor and approved by the agency (e.g., the OVF standard could be a partial basis for such a strategy).

(4) **Virtualization Best Practices.** The Contractor shall follow best practices for the administration of conventional systems and networks, and for use of virtualization (i.e., NIST Guide to Security for Full Virtualization Technologies SP 800-125).

(5) **Identity and Access Management.** The Contractor shall provide DOI visibility into to the following capabilities of the provider:

a. the authentication and access control mechanisms that the provider infrastructure supports;
b. the tools that are available for subscribers to provision authentication information; and
c. the tools to input and maintain authorizations for subscriber users without the intervention of the provider.

(6) **Visibility.** The Contractor shall provide DOI visibility into the operating services that affect a specific agency subscriber's data or operations on that data.

(7) **Virtual Machines (VM) Vulnerabilities.** The Contractor's computing resources offered in the form of VMs, shall include mechanisms provided by the provider to protect VM attacks from:

a. other VMs on the same physical host;
b. the physical host itself; and
c. network originated attacks.

Typical attack detection and prevention mechanisms include Virtual Firewalls, Virtual IDS/IPS, and network segmentation techniques such as VLANs.

VM image templates shall only be shared, made available for reuse, or implemented when designed from scratch and in a secure manner that prevents the possibility of any pre-existing authentication credentials or decryption keys from being inadvertently shared or used for unintended or unauthorized purposes. VM image templates shall also be updated to incorporate the most current secure configurations and security patch levels as also required of VM production images already deployed and operating. These requirements are to address the risks inherent in trusting VM image templates to be free of backdoors, trojans, and other malicious code.

11.6.2 INDEPENDENT VERIFICATION AND VALIDATION (IV&V)

In the development or maintenance of custom applications, software shall be independently verified and validated using a methodology determined appropriate by the DOI System Owner prior to being moved into production.

Contractor will ensure that IV&V, as deemed appropriate by the DOI System Owner, is performed on software deployed on Provider managed systems containing DOI data/information, in accordance with the methodology specified by the DOI System Owner.

11.6.3 INTERNET LOGON BANNER

A Government-approved logon banner must be displayed on the first page of any public access web pages.

11.6.4 LOGON WARNING BANNER

Contractor employees who will access DOI data/information must acknowledge a Government-approved logon warning prior to each logon to the system.

11.6.5 QUALITY CONTROL (MALICIOUS CODE)

All software and hardware shall be free of malicious code.

11.6.6 SECURITY CONTROLS

In the development or maintenance of custom applications, the Provider shall, with the knowledge and concurrence of the DOI System Owner, be responsible for IT security for all non-government-owned systems used in the development of, and systems intended for eventual delivery to, DOI in fulfillment of contract requirements. This includes IT, hardware, software, databases, networks, and telecommunications systems.

Security functionality in applications or integrated systems delivered hereunder must operate with the Government systems on, or with, which it will eventually be deployed. Products delivered hereunder must not cause misoperation of government resources or loss of confidentiality, integrity or availability of electronic information or data.

The Provider shall ensure compliance with the security control requirements of the current version of NIST FIPS Pub 200 and SP 800-53 and correspond to the information system potential risk impact ratings of "LOW", "MODERATE" or "HIGH" for the Confidentiality, Integrity and Availability objectives, and overall "LOW", "MODERATE" or "HIGH" information system security categorizations, commensurate with DOI's hosted information and information systems and the associated FCHS IaaS, PaaS and SaaS information systems as DOI has determined based on FIPS Pub 199 and SP 800-60.

The Provider shall be responsible for IT security for all contractor-operated systems connected to a DOI network, regardless of location. The Contractor shall ensure compliance with the security control requirements of current version of NIST FIPS Pub 200 and SP 800-53 and appropriate to the sensitivity and criticality of the application/system.

11.6.7 TRAINING

Provider employees must complete DOI's end-user computer security awareness training, or equivalent, prior to being granted access to DOI data or being issued a user account. Training must be renewed annually. Provider employees are also required to annually complete IT security role-based training in accordance with the NIST SP 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model*, and DOI's Role-Based Security Training (RBST) Standard. The Provider shall annually prepare a report listing all Provider employees, security awareness course completion status by each employee, and IT security role-based training completion status by each employee with an explanation as to how each employee satisfied these annual training requirements. The Provider shall maintain records of all supporting evidentiary artifacts of completion and make them available for inspection/audit by the government upon request.

11.6.8 PRIVACY

11.6.8.1 USE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

The Contractor shall comply, and cause Provider to agree to at all times, with all requirements outlined herein to protect the Government's information and data. Neither the Contractor nor Provider shall use any PII, Email Groups, Lists, or contact information for any purpose other than those activities necessary for the performance of this contract.

11.6.8.2 TRANSFER OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personal information collected or otherwise processed by Contractor shall be accessed, transferred, stored or processed only within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands). The primary locations shall be the primary and back-up facilities located within the sole jurisdiction of the United States Federal Government (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the Virgin Islands). In addition, other sites include the location of teams who provide support to DOI in resolving issues regarding the email and collaboration solution, locations where backup or archiving facilities may be agreed to by DOI, or sites where antivirus and other security scans are performed. To the extent that material changes are made the Contractor shall use a mutually agreed upon Change Management Process to notify DOI.

12. ROLES AND RESPONSIBILITIES

12.1 Authorizing Official

The authorizing official is the DOI Chief Information Officer (CIO). The DOI CIO formally assumes all risks to DOI for use of these external information services.

The authorizing official is responsible for:

- Reviewing and approving the security requirements, information security documentation, and CMP.
- Approving the authorization to operate (ATO).
- Reviewing risk reports on an ongoing basis.
- Disapproving the ATO if the trust relationship with the service provider is broken.

The authorizing official may rescind the authorization to operate immediately if an acceptable level of trust and applicable controls are not maintained, which may result in termination of the contract.

12.2 Information Owner

The information owner is the DOI official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information service. This is typically the management official who funds the acquisition for the system.

The information owner is responsible for:

- Ensuring a privacy impact assessment is performed.
- Ensuring a security categorization is performed.
- Ensuring the service provider assesses and implements all applicable controls.
- Ensuring that continuous monitoring is being performed.
- Reporting risk to the authorizing official as defined in the CMP.

Service Provider

The service provider is the third-party entity hired by the information owner to provide services external to the DOI network of services.

The service provider is responsible for:

- Collaborating with the information owner to implement all applicable controls.
- Performing continuous monitoring activities.
- Sharing information as required by the CMP.

13. IT Security Policies, Standards, Guidelines and Other Publications

One or more of the following sources of requirements relating to IT security and privacy have been incorporated by reference into the solicitation/statement of objectives. Copies of documents cited herein can be obtained as described below.

The following documents may be accessed electronically at these addresses:

- Office of Management and Budget (OMB) Circulars, Memoranda and Bulletins: http://www.whitehouse.gov/omb/memoranda_default
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publications and 800 Series Special Publications (SP): http://csrc.nist.gov/publications/PubsSPs.html;
- National Institute of Standards and Technology (NIST) Security Technical Implementation Guides (STIGs – also referred to as security configuration checklists): http://web.nvd.nist.gov/view/ncp/repository
- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance: http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf
- DOI Privacy Impact Assessment (PIA): http://www.doi.gov/archive/ocio/privacy/pia.html

Certain DOI documents are not publicly available. If one of these documents has been referenced elsewhere in this solicitation, it will be provided to interested Offerors under an appropriate non-disclosure agreement (NDA) upon receipt by the Contracting Officer of a written request signed by a responsible official of that organization.

[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

APPENDIX A

IT Security and Privacy Checklist

For External Information System Services

Step 1: Privacy Impact Assessment (DOI Responsibility)
The information owner is required to complete a Privacy Impact Assessment to identify if there is any Personally Identifiable Information (PII) being generated, stored, processed, or exchanged by the system.

Step 2: Security Categorization (DOI Responsibility)
The information owner is required to categorize the system and the information processed, stored, or transmitted by the system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and document the results (including supporting rationale) in the system security plan.

Step 3: Information Security Documentation (DOI & Service Provider Responsibility)
The service provider is required to develop and maintain system security documentation that reflects the current security posture of the information system. The information security documentation and the required content are determined by NIST standards and *DOI Security Control Standards*.

Step 4: Security Assessment (DOI & Service Provider Responsibility)
The service provider is required to perform a security assessment, using a trusted independent assessor, by assessing the controls identified in the *DOI Security Control Standards* and ensuring the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements.

Step 5: Authorization to Operate (DOI & Service Provider Responsibility)
The DOI Authorizing Official must approve the ATO. The ATO is a formal declaration by the authorizing official that an information service is approved to operate in a particular security mode, using a prescribed set of safeguards and at an acceptable level of risk.

Step 6: Continuous Monitoring (DOI & Service Provider Responsibility)
The information owner and service provider are required to maintain the security level of the system over time by implementing and monitoring the security controls identified in the *DOI Security Control Standards,* and the supporting CMP, on an ongoing basis.

APPENDIX B

Deliverable and Reporting Requirements

Deliverables and Reports:

Title	Description	Due Date/Frequency	Government Approval and Surveillance
Information Assurance (IA) Documentation	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO) (COR)
System Security Plan (SSP)	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document..	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Continuous Monitoring Plan (CMP)	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Preliminary Privacy Impact Analysis (PIA - Privacy Threshold Analysis (PTA))	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Privacy Impact Analysis (PIA)	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Contingency Plan	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)

Title	Description	Due Date/Frequency	Government Approval and Surveillance
Independent Assessor's Security Assessment Plan and Report (SAP/SAR)	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Plan of Action and Milestones (POA&M)	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Upon Completion prior to authorization to move to Service Ready status and Quarterly Thereafter	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Vulnerability and Security Configuration Scan Report	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Monthly	Contracting Officer's Representative (COR), Government system owner
Continuous Monitoring Report	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Monthly	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Independent Penetration Testing and Report	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	Annually	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Documentation for Audit Requirements	As described in, and in accordance with, the FCHS IT Security and Privacy Requirements document.	30 calendar days after written request	Contracting Officer's Representative (COR), Government system owner, Government Authorizing Official (AO)
Training Compliance Report	As described in, and in accordance with, theFC IT Security and Privacy Requirements document.	Annually	Contracting Officer's Representative (COR), Government system owner
Security Incidents	As described in, and in accordance with,	Per Incident (immediately but not	Contracting Officer (CO), Contracting Officer's

Title	Description	Due Date/Frequency	Government Approval and Surveillance
	the FCHS IT Security and Privacy Requirements document.	more than 2 hours)	Representative (COR), Government system owner, Government Authorizing Official (AO), DOI-CIRC
Contractor Employee Report	Report of all contractor employees that have access to DOI Data with status of required background checks as specified.	Annually on contract award anniversary date and within 3 business days upon written request	Contracting Officer's Representative (COR)

United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240

SEP 2 1 2007

TAKE PRIDE IN AMERICA

Memorandum

To: Bureau and Office Chief Information Officers
Bureau and Office Privacy Officers
Chief Financial Officer
Solicitor
Inspector General
Chief Information Security Officer
Legislative Affairs Officer

From: Michael J. Howell
Chief Information Officer and
Senior Agency Official for Privacy

Subject: Departmental Privacy Loss Mitigation Strategy

This Strategy incorporates the Office of Management and Budget (OMB) recommendations and guidelines for safeguarding personally identifiable information (PII), reducing incidents of breach and establishing a breach notification policy.[1] As noted in the Strategy, the Department of the Interior formed a Departmental Identity Theft Task Force (ITTF) with a standing team of senior officials as members that meet on an ad hoc basis to develop Departmental policy, revise this Strategy as necessary, address Department level breaches of PII and monitor Bureau and Office compliance with OMB guidelines related to PII. Bureaus and Offices should form their own Identity Theft Task Forces (BITTFs) to address breach incidents and to assist with safeguarding PII, by October 12, 2007. Bureaus and Offices are encouraged to adopt this strategy to the extent practicable and only augment it to meet their specific situations and needs.

Copies of the Strategy and Charter will be sent to those bureaus and offices that do not have internet access. Please contact Miriam Lam at (202) 208-3588 or by email at Miriam_Lam@ios.doi.gov if you have questions.

Attachments:
Privacy Loss Mitigation Strategy
Departmental Identity Theft Task Force Charter

---

[1] See "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," (OMB Memorandum M-07-16) issued May 22, 2007 at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

Department of the Interior

Identity Theft Task Force Charter

Version 1.0

--- This Page Intentionally Left Blank ---

Table of Contents:

1.0 Background 2
2.0 Identity Theft Task Force Membership 2
3.0 Identity Theft Task Force Responsibilities 3
4.0 Meetings and Scheduling 4
5.0 Definitions 5
6.0 Acceptance 6

1.0 Background

Safeguarding Personally Identifiable Information (PII) in the possession of the government and preventing its breach is essential to ensure the government retains the trust of the American public. On May 10, 2006 the President established the Identity Theft Task Force by Executive Order 13402 to strengthen Federal efforts to protect against identity theft. In support of this effort, the Office of Management and Budget (OMB) has defined requirements for the development and implementation of Federal agency breach notification policies and guidelines for safeguarding PII.

One of the requirements defined by OMB is the establishment by each Federal agency of an agency response team. This team is responsible for defining the policies and procedures that will govern responses to breaches of PII that occur within the span or control of the Department. The team is also responsible for implementing the policies and procedures in response to individual incidents of PII breaches. This document defines the specific responsibilities of Interior's Identity Theft Task Force (ITTF) in order to meet the requirements for an agency response team as defined by OMB.

The mission of the ITTF is to provide advance planning, policy, breach incident coordination and guidance regarding the actual and potential breaches of PII within the custody of the Department. The ITTF will meet on an ad hoc basis to address incidents of breach and to update the Privacy Loss Mitigation Strategy pursuant to newly issued memoranda from OMB, Office of Personnel Management (OPM)[1] or pursuant to the Federal Information Security Management Act (FISMA) which require agency action.

In the event of a breach, the Interior ITTF serves as liaison and decision making body between the functional area(s) affected and other organizations and Bureau/ Office ITTFs (BITTFs).[2] Liaison services include the support provided by DOI Computer Incident Response Center (DOI-CIRC) incident response teams, Office of the Inspector General (OIG), Office of Management and Budget (OMB), United States Congress, and public information dissemination handled by Public Affairs, among others.

2.0 Identity Theft Task Force Membership

The ITTF will be comprised of the following Department of the Interior officials as permanent core members[3]:

- Senior Agency Official for Privacy (SAOP) (Acts as Chairperson or designates an alternate as the Chairperson)

---

[1] *See* OPM Memorandum, "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft," issued June 18, 2007 at http://www.chcoc.gov/Attachments/trans847.pdf.

[2] The duties of the Bureau/ Office ITTFs (BITTFs) are outlined in the Departmental Privacy Loss Mitigation Strategy, issued in September 2007 by the Office of the Chief Information Officer. As noted in that Strategy, Bureaus and Offices may use this Charter as template for establishing their BITTFs.

[3] See OMB Memorandum, "Recommendations for Identity Theft Related Data Breach Notification," issued September 20, 2006 at http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

- Departmental Privacy Officer
- Chief Information Officer (CIO)[4]
- Chief Financial Officer (CFO)
- Solicitor
- Inspector General (IG)
- Chief Information Security Officer (CISO)
- Legislative Affairs Officer

3.0 Identity Theft Task Force Responsibilities

The Interior ITTF is responsible for:

- Defining policies and procedures for protecting PII and preventing identity theft.
- Defining policies and procedures for responding to breaches of PII.
- Reviewing policies and procedures on a regular basis and making updates to policies and procedures as appropriate.
- Determining appropriate responses to incidents of PII breaches, following the policies and procedures that have been defined (referred from BITTFs).

Initially the ITTF will be responsible for finalizing, approving and issuing a Departmental Privacy Loss Mitigation Strategy.

In order to fulfill its responsibilities, the ITTF will coordinate with other DOI offices such as Human Resources, Bureau/Office Chief Information Officers, Bureau/Office Privacy Officers, the Office of Law Enforcement and the Office of the Inspector General Cyber Crimes Investigative Unit. Additionally, the ITTF will work closely with other Federal agencies, and teams as needed.

Assignments will be made within the ITTF for developing specific work products such as draft policies and procedures. The ITTF Chairperson may assign action items to ITTF members or their organizations. The task force may appoint temporary project working groups to address specific issues.

Approval of additions, deletions, or modifications to Departmental PII breach incident handling policy, procedures, standards, or technical guidelines will be determined based on collaboration and consensus, or when necessary, by a majority.

The ITTF will establish processes for approval and promulgation of new and updated policies relating to PII and identity theft.

---

[4] Current DOI policy assigns the role of Senior Agency Official for Privacy (SAOP) to the Chief Information Officer. The two roles are defined separately in this document in the event that the role of SAOP is filled by someone other than the CIO at some point in the future.

4.0 Meetings and Scheduling

Task force teleconference meetings will be held on a bi-monthly basis. Other meetings may be called by the Senior Agency Official for Privacy or task force members if deemed necessary to respond to specific incidents involving PII or fulfill the ITTF duties listed above in section 3.0. When possible, face-to-face meetings are to be held on a quarterly basis and in synchronization with the FISAM Quarterly Report. ITTF meeting criteria will include:

- **Agenda:** The ITTF Chairperson will distribute the agenda prior to each meeting via email or fax. Possible agenda items for future meetings will be collected at the end of each meeting, but may also be submitted electronically prior to the next meeting. Sensitive issues and materials will be handled appropriately.

- **Conduct:** Meetings will be structured, adhere to the published agenda, and follow recognized meeting behavior (e.g., respect, listening, sharing, courtesy, etc.).

- **Chairperson:** The ITTF Chairperson will provide the deciding vote in the event of a tie, and act immediately on urgent requirements by polling task force members by phone, email, or fax.

- **Recording Secretary:** The ITTF will select a recording secretary who will record meeting minutes, requirements and action items. The recording secretary will provide written minutes and an action item report to all members within two working days of each meeting. The recording secretary may be a member of the task force.

5.0 Definitions

Access: The ability or opportunity to gain knowledge of personally identifiable information.

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to personally identifiable information in usable form, whether physical or electronic. A breach would not occur if, for example, the information was properly encrypted within a mobile computing device because the information would be unusable.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to a specific individual.

Privacy: Freedom of an individual from intrusion or observation; the right to maintain sole control over PII; and the expectation that others will respect the individual's rights.

Professional Need to Know: Specific and limited information necessary to complete assigned work, in the case of performing official business.

Security: Administrative, physical and technical safeguards, used to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration or destruction, to maintain the integrity of the information.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Mitigation: To make less severe, to partially remove, or to correct, so that harmful effects of an incident are reduced or eliminated.

Violation: Infraction of a law; going against established rules.

6.0 Acceptance

_____
Senior Agency Official for Privacy (SAOP)

_____
Departmental Privacy Officer

_____
Chief Information Officer (CIO)

_____
Chief Financial Officer (CFO)

_____
Solicitor

_____
Inspector General (IG)

_____
Chief Information Security Officer (CISO)

_____
Legislative Affairs Officer

_____
DATE

Attachment 3

Department of the Interior

Privacy Loss Mitigation Strategy

Version 1.0

--- This Page Intentionally Left Blank ---

Table of Contents:

1.0 Introduction 1
1.1 Document Organization 2
1.2 Intended Audience 2
2.0 Design of the Strategy 3
2.1 Overview of the Privacy Loss Mitigation Strategy 3
2.2 Identity Theft Task Force 3
2.3 Assumptions 4
2.4 Development 5
2.5 Maintenance 5
2.6 Testing 5
3.0 Privacy Loss Mitigation Strategy 6
3.1 Privacy and Security Requirements – A General Overview 7
3.2 Rules and Consequences 10
3.3 Bureau and Office Information Technology Security and Privacy Programs 11
3.4 Types of Breaches: Incidental, Accidental, and Intentional 12
3.5 Detection of a breach 14
3.6 Requirements for reporting breaches of PII 16
3.7 Breach Incident Reporting and Handling Procedures 17
3.8 Incident Response Checklist 18
3.9 Perform Initial Assessment of Incident 19
3.10 Confirm Completion of Appropriate Internal Notifications 19
3.11 Confirm Involvement of Appropriate Personnel 19
3.12 Determine Exact Nature of the breach 19
3.13 Analyze PII Involved to Determine Potential Impact 19
3.14 Determine Mitigation Plan of Action 19
3.15 Complete Mitigation Plan of Action and External Notification 21
3.16 Review Lessons Learned 21
4.0 External Breach Notification 22
4.1 External Notification Determining Factors 22
4.2 Whether Breach Notification is Required 22
4.3 Timeliness of Notification 23
4.4 Source of Notification 23
4.5 Contents of Notification 23
4.6 Methods of Providing Notification 24
4.7 Notification of Third Parties 25
Appendix A 26
DOI Missing IT Asset Impact Analysis Form 26
Appendix B 28
General Guidance for the Establishment of a Call Center in the Event of a Privacy Act Breach 28
Appendix C 33
Sample Written Notification 33
SAMPLE LETTER 1 33
SAMPLE LETTER 2 34

SAMPLE LETTER 3 35
SAMPLE NEWS RELEASE 36
Appendix D 37
Bureau/Office Identity Theft Task Force Strategy Flowchart 37
Appendix E 38
Definitions 38

1.0 Introduction

The Department of the Interior (DOI) Senior Agency Official for Privacy (SAOP), with assistance from key Department support areas, is responsible for developing the Department's Privacy Loss Mitigation Strategy in accordance with Office of Management and Budget (OMB) Memoranda on "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006[1] and "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (M-07-16)," issued on May 22, 2007.[2] Overall, this Privacy Loss Mitigation Strategy focuses on actions that the Department will take to safeguard personally identifiable information (PII)[3] that it is maintained in various formats (*e.g.*, paper, electronic, etc.) by the Department.[4]

The Privacy Loss Mitigation Strategy addresses ways in which the Department can reduce the potential for harm from breaches involving PII and steps that will be taken if a breach occurs. Detailed in this Strategy is a breach notification policy[5] that incorporates the existing privacy and security requirements regarding PII that apply to all Federal information and information systems.[6] This Strategy further outlines the existing and new requirements for reporting and handling incidents of breach involving PII. In addition, this Strategy addresses the responsibilities and duties of Departmental personnel that are authorized to access PII.

This Strategy is provided in three major sections as follows: (1) an overview addressing the design of the Strategy; (2) the Privacy Loss Mitigation Strategy; and (3) External Breach Notification policy.

---

[1] *See* http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

[2] *See* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf (Hereinafter OMB M-07-16).

[3] *Id* at 1. ("Personally identifiable information" is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as a date and place of birth, mother's maiden name, etc.)

[4] This strategy supplements DOI Office of the Chief Information Officer Directive issued in September 2007 and titled, "Departmental Strategy to Safeguard Personally Identifiable Information and Reduce the Collection and Uses of Social Security Numbers," that addresses the departmental strategy safeguard personally identifiable information and social security numbers.

[5] *See* OMB M-07-16 at 1. (According to OMB M-07-16, in the breach notification policy that agencies are required to develop and implement, "the term 'breach' is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic... 'access' means the ability or opportunity to gain knowledge of personally identifiable information.")

[6] *Id.* (The security requirements referred to OMB M-07-16 are requirements established by the Federal Information Security Management Act (FISMA) of 2002 and apply to Federal information and information systems.)

1.1 Document Organization

1. Design of the privacy loss plan that this document records, includes information about the overall structure of the Privacy Loss Mitigation Strategy at DOI and Bureau/ Office roles.

2. General responsibilities of the individual Department support teams that together form the Interior Identity Theft Task Force, emphasizing functional roles and preparation responsibilities.

3. External breach notification policy of individuals affected, and third parties when applicable, of a breach involving PII.

4. Recovery actions for the Department support teams and important checklists such as the notification list for a breach and an inventory of resources required for response.

1.2 Intended Audience

This document addresses several groups within Interior by detailing the various internal controls and the types of responsibilities related to the protection of PII. These groups include:

- Administrative and Policy teams
- Interior and Bureau Identity Theft Task Forces
- Bureau and Office Information Technology Security and Privacy Programs
- Interior Incident Response Program Offices

2.0 Design of the Strategy

2.1 Overview of the Privacy Loss Mitigation Strategy

DOI increasingly depends on computer-supported information processing and telecommunications. This dependency will continue to grow with the trend toward decentralizing information technology to individual organizations within DOI. The increasing dependence on computers and telecommunications for operational support, combined with an increasing amount of information being collected by government systems, poses a potential risk of significant loss of privacy information that seriously impacts the operations of the Department.

Interior recognizes the potentially significant risks associated with the loss of privacy information. The potential for significant impact to affected individuals necessitates that Interior develop and maintain a plan that mitigates the risk of damage resulting from a loss of privacy information. The Department's Privacy Loss Mitigation Strategy is designed to reduce the risk and impact of a breach involving PII by ensuring the implementation of appropriate safeguarding measures and the development and implementation of policies for breach notification and appropriate handling of PII.

The Privacy Loss Mitigation Strategy identifies the critical functions of DOI and the resources required to support them. This Strategy provides guidelines for ensuring that necessary personnel and resources are available both to prepare for and respond to a breach. This Strategy also details the proper steps that will be taken to permit the timely notification of individuals impacted by breaches of PII.

2.2 Identity Theft Task Force

This Privacy Loss Mitigation Strategy specifies the responsibilities of the Interior Identity Theft Task Force (ITTF) and the Bureau/Office Identity Task Forces (BITTFs) in safeguarding PII collected, used and maintained by the Department. The mission of the ITTF is to provide advance planning, policy, breach incident coordination and guidance regarding the actual and potential breaches of PII within the custody of the Department. The ITTF will meet on an ad hoc basis to address incidents of breach and to update this Strategy pursuant to newly issued memoranda from OMB, Office of Personnel Management (OPM)[7] or pursuant to the Federal Information Security Management Act (FISMA) which require agency action. The ITTF will be comprised of the following DOI officials[8]:

- Senior Agency Official for Privacy (SAOP) (Acts as Chairperson or designates an alternate as the Chairperson)
- Departmental Privacy Officer
- Chief Information Officer (CIO)

[7] *See* OPM Memorandum "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft," issued June 18, 2007 at http://www.chcoc.gov/Attachments/trans847.pdf.
[8] *See* OMB Memorandum, "Recommendations for Identity Theft Related Data Breach Notification," issued September 20, 2006 at http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

- Chief Financial Officer (CFO)
- Solicitor
- Inspector General (IG)
- Chief Information Security Officer (CISO)
- Legislative Affairs Officer

The membership of the BITTFs will be determined by bureau CIOs but must include:

- Bureau/ Office Chief Information Officers
- Bureau/ Office Privacy Officers
- Bureau/ Office IT Security Managers

In the event of a breach, the Interior ITTF serves as liaison and decision making body between the functional area(s) affected and other organizations and BITTFs. As BITTFs are established, thresholds will be defined by the Department to determine any significant breaches that will be elevated to the Departmental level.[9] Liaison services include the support provided by DOI Computer Incident Response Center (DOI-CIRC) incident response teams, Office of the Inspector General (OIG), Office of Management and Budget (OMB), United States Congress, and public information dissemination handled by Public Affairs, among others. Attached to this Strategy is a Charter establishing the Interior ITTF. Bureaus and offices may use this Charter as a template for establishing their BITTFs.

2.3 Assumptions

This Strategy is predicated on the validity of the following three assumptions:

1. The situation that causes the breach of PII of data is localized to Interior systems, for which Interior is wholly responsible. It is not a general loss, such as a compromise of a commercial entity like "ChoicePoint", a leading provider of identification and credential verification services for business and government, which affects a broader category of entities that includes DOI. (It should be noted however, that the Strategy will still be functional and effective even in a general loss circumstance.)

2. This Strategy reflects the changing environment and requirements of DOI. Therefore, it requires the continued allocation of resources to maintain it and to keep it in a constant state of readiness.

[9] Regardless of the Task Force level of review, all instances in which an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource or if there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred must be reported to the US-Computer Emergency Readiness Team (US-CERT) – (see Section 3.7 of this Strategy for those reporting guidelines). (See OMB Memorandum, "Recommendations for Identity Theft Related Data Breach Notification," issued September 20, 2006 at http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.)

3. The notification required by the Strategy may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

2.4 Development

Interior's Senior Agency Official for Privacy (SAOP), with assistance from key Department support areas, is responsible for developing the Department's Privacy Loss Mitigation Strategy. Development and support of individual Bureau Privacy Loss Mitigation Strategies are the responsibility of the functional area planning for recovery.

2.5 Maintenance

Ensuring that the Strategy reflects ongoing changes to resources is crucial. The Interior ITTF is responsible for maintaining this document. Such maintenance includes routine updates and revisions to the Strategy pursuant to future memoranda and policy requirements as determined by Federal entities such as OMB, OPM, etc., with regard to PII, testing the updated Strategy, and training personnel and to define thresholds for significant breaches as they are to be reviewed by the ITTF.

Quarterly and Annual Reviews

In addition to updating and revising the Strategy to comply with any applicable, newly implemented Federal guidelines, the Interior ITTF will review the Strategy on a quarterly basis (synchronized with the FISMA Quarterly reporting schedule) to ensure that it adequately addresses Departmental issues concerning breaches of PII. Revisions will be distributed to Bureau/ Office Chief Information Officers and Bureau ITTF Leads. The Senior Agency Official for Privacy (SAOP) will request an annual status report on Privacy Loss Mitigation planning from the Interior ITTF.

2.6 Testing

Testing the Privacy Loss Mitigation Strategy is an essential element of preparedness – hence, partial tests of individual components and mitigation plans of specific Bureau/ Office teams may be expected to be carried out on a regular basis. A comprehensive exercise of our Privacy Loss Mitigation capabilities and support will be performed on an annual basis.

3.0 Privacy Loss Mitigation Strategy

The Department of the Interior promotes ethical standards of conduct and encourages all members of its workforce and the workforce of its affiliated entities to honor the privacy rights of individuals, including compliance with the Privacy Act of 1974. The Privacy Loss Mitigation Strategy pertains specifically to a breach involving PII.[10]

In order to help prevent a breach of PII, there are a number of steps that personnel can take to better safeguard PII. For example, any individual overhearing a conversation openly discussing, and either intentionally or unintentionally disclosing, PII related to a third party or other sensitive agency information where unauthorized individuals have the potential to overhear that information, should politely remind all involved parties that the discussion is in violation of Departmental policy regarding the protection of PII and sensitive agency information. The person overhearing this conversation should then report the occurrence to their Bureau/Office Privacy Officer for resolution and follow-up as appropriate. In other cases where documents containing PII are discovered in a public place, they should be returned to the Bureau/ Office Privacy Officer. Also, one should take steps to physically secure or lock up an area or equipment with accessible PII.

In the event that a breach does occur, however, procedures are required to adequately address that situation. According to DOI- Computer Incident Response Center (CIRC) procedures (as defined more specifically in this Strategy, Sections 3.5 and 3.6), a party that detects or suspects an unauthorized disclosure or acquisition of PII, must first immediately report the incident to (a) the appropriate Bureau/Office Privacy Office in question, as well as the immediate supervisor (b) the Bureau IT Security Manager (BITSM), and (c) the relevant BITTF Lead. The Bureau/Office CIO and BITTF will then report this incident to the Departmental Privacy Officer and Interior ITTF Lead. All incidents involving PII will be investigated independently. If confirmed, the Department will recommend corrective actions and sanctions, and will try to mitigate, to the extent possible, any harmful effect of a confirmed incident.

The Bureau/ Office ITTF's will make reasonable efforts to notify affected persons if it is determined that there has been a breach involving their PII. (See Section 4.0, External Breach Policy and Appendix C of this Strategy for sample notifications to individuals affected by the breach.) In all cases, the relevant bureaus, offices, or other departmental units from which the PII was acquired will be responsible for the costs and labor associated with notifying affected persons.

As noted before, as Bureau ITTFs are established, thresholds will be defined by the Department to determine those significant breaches that will be elevated to the Departmental level. As noted in Section 2.5 "Maintenance", routine updates and revisions to this Strategy may be made to further refine these distinct functions.

---

[10] *See* footnote 3 for the OMB Memorandum 07-16 definition of PII.

This section addresses the following phases associated with addressing PII loss:

- Reporting
- Investigating
- Responding

3.1 Privacy and Security Requirements – A General Overview

Under existing law, executive orders, regulations, and policy, agencies must comply with a number of privacy and security requirements to appropriately safeguard PII.[11] In particular, pursuant to the Privacy Act of 1974[12], existing privacy requirements include the following:

- Establishing Rules of Conduct "for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of the [Privacy Act], including any other rules and procedures adopted pursuant to the [Privacy Act] and the penalties for non-compliance"[13];

- Establishing "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained"[14];

- Maintaining PII in a system of records (including through the use of notices to the public), and other information considered PII in a manner that is accurate, relevant, timely and complete including through the use of notices to the public[15]; and

- Ensuring that personnel responsible for handling, collecting or accessing PII maintained in Privacy Act Systems of records is fully aware that the Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency without the written consent of the subject or individual unless the disclosure falls within one of the twelve statutory exceptions. Other PII not maintained in

[11] OMB M-07-16, Attachment 1.
[12] 5 U.S.C. § 522a.
[13] 5 U.S.C. § 522a(e)(9).
[14] 5 U.S.C. § 522a(e)(10).
[15] 5 U.S.C. § 522a(e)(4); See also OMB Memorandum 07-16 for definition of PII.

Privacy Act systems should be handled according to OMB safeguards and requirements.

Existing Requirements – OMB Memorandum M-07-16

Existing security requirements with which agencies have been required to comply include the following:

- Assigning an impact level to all information and information systems following the processes outlined in the Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," which categorizes all information and information systems using three levels of impact (i.e., low, moderate, or high). *Agencies should generally consider categorizing sensitive PII (and information systems in which such information resides) as moderate or high impact*[16];

- Implementing minimum security requirements and minimum (baseline) controls set forth in FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," and National Institute for Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems";

- Certifying and accrediting (C&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor or other source[17];

- Training employees, including managers on their privacy responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training must be provided commensurate with increased responsibilities or change in duties. Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing telework and other authorized remote access programs, training must also include the rules of such programs.

[16] OMB M-07-16, Attachment 1(B)(2)(a).
[17] 44 U.S.C. § 3544(b).

New Requirements – OMB Memorandum M-07-16

In order to appropriately safeguard PII and Social Security numbers (SSNs) that an agency collects or maintains, there are new privacy and security requirements with which agencies are expected to comply.[18] These new requirements include:

- Reviewing current holdings of all PII and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.

  Following an initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agencies annual review of and any consolidated publication of minor changes of Privacy Act systems of records notices.

- Reducing the use of Social Security Numbers (SSNs) in agency systems and programs and identify instances in which collection or use of the SSNs is superfluous. Agencies must also explore alternatives to use of SSNs as personal identifiers for Federal employees and in Federal programs (i.e. data calls, surveys, etc.).

- Ensuring that an agency is able to respond in a timely and effective manner in accordance with the Privacy Act[19], agencies should publish a routine use for appropriate systems to specifically allow for disclosure of information in connection with response and remedial efforts in the event of a data breach.[20]

Interior and other agencies continue to be responsible for implementing existing security policies and National Institute of Standards and Technology (NIST) guidance. Pursuant to OMB memoranda, M-06-16, "Protection of Sensitive Agency Information" and OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," the following are five security requirements that Interior is responsible for implementing:

- Encryption- using only NIST certified cryptographic modules encrypt all data on all mobile computers and devices that carry sensitive data (non-sensitive data should be designated as such in writing by the Deputy Secretary or their designee – currently delegated to the Department's CIO and may not be delegated further);

[18] See OMB M-07-16, Attachment 1(B) and (C).
[19] 5 U.S.C. § 522a(b)(3).
[20] See OMB Memorandum M-07-16, Attachment 2, B.2.

- Control Remote Access- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

- Time-out function- Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of computer inactivity;

- Log and Verify- Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days of its use is still required;

- Ensure Understanding of Responsibilities- Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities; and

- Establishing Agency wide best practices- informing employees of Agency's low tech safety measures they can use to ensure protection of PII (such as using privacy screens when working outside the office or packing laptops in carry-on luggage rather than checked baggage when traveling).

3.2 Rules and Consequences

Neither the Department of the Interior, nor any of its employees or business associates, shall discipline, or take any other adverse personnel action against an employee for:

- Reporting a violation or suspected violation of any federal, state, or local law, rule or regulation committed by an employee or business associate of the Department; or

- Participating in an investigation, hearing, or other inquiry conducted by any agency of the federal government.

Members of DOI's workforce who fail to comply with the Department's privacy policies and procedures or with the requirements of federal privacy regulations will be disciplined in accordance with the Department of the Interior's normal disciplinary procedures, up to and including termination of employment. (*See* DOI Personnel Management Departmental Manual Section 370 DM 752 [Appendix B(2)]; "Discipline and Adverse Actions", ; DOI Privacy Act Manual Section, 383 DM 9.7, "Employee Handling of Privacy Act Records" and 5 U.S.C. § 552a(i)(1)).

Members of DOI's affiliated entities' workforce who fail to comply with applicable DOI privacy policies and procedures or with the requirements of federal privacy regulations

will be disciplined in accordance with that entity's normal disciplinary procedures, up to and including termination of employment. (*See* DOI Personnel Management Departmental Manual Section 370 DM 752 [Appendix B(2)] ,"Discipline and Adverse Actions,"; DOI Privacy Act Manual Section, 383 DM 9.7, "Employee Handling of Privacy Act Records" Investigations and Disciplinary Action: The Senior Agency Official for Privacy or designee monitors investigations and corrective actions performed by the Bureau/Office in which the incident occurred. The SAOP may recommend sanctions in consultation with the ITTF and BITTFs for confirmed violations.

In deciding what action to take for violations of this policy, the following factors are considered:

- The nature of the violation,
- The severity of the violation,
- Whether the violation was intentional or unintentional, and
- Whether the violation indicates a pattern or practice of improper use or disclosure of PII.

Depending on the circumstances and impact of the violation, corrective action may include verbal warning, reprimand, suspension, removal, or separation from employment in accordance with applicable law and agency policy. As noted in Section 2.5 "Maintenance," routine updates and revisions to this Strategy may be made to further refine distinct actions with relation to the categories above as further policies evolved with regard to protection and mitigation of PII.

All privacy-related sanctions that are applied by the Department of the Interior will be documented in the employee's personnel file.

3.3 Bureau and Office Information Technology Security and Privacy Programs

The Interior ITTF provides overall direction to the Bureau and Office Information Technology Security and Privacy Programs (ITSPPs) and provides support to assist offices and bureaus impacted by a breach as well as sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies. These ITSPP teams work to mitigate problem conditions and provide assistance at the Department level during the initial stages of a breach involving PII. For breaches, the team reports directly to the DOI-CIRC, and evaluates the initial status of the breach, and estimates both the severity of the incident and its potential for harm.

Bureau and Office ITSPPs are required to respond to a breach, or to a problem that could evolve into a breach, by:

1. Detecting and determining a breach condition for their respective community;

2. Immediately notifying DOI -CIRC, the OIG, and other applicable parties of a potential breach;
3. Initiating the Department's Privacy Loss Mitigation Strategy;
4. Following ITTF guidance on significant breaches;
5. Disseminating ITTF approved and appropriate Public Information and Notifications; and
6. Providing support services to aid recovery.

3.4 Types of Breaches: Incidental, Accidental, and Intentional

The personnel responsible for the maintenance, safeguarding and handling of PII should be aware that there are different types of breaches that involve PII. These types of breaches include:

- *Incidental Disclosures*: Unintentional disclosures of PII that occur as a result of the normal course of business, and which are incidental to an otherwise permitted use or disclosure of the information.

  If a member of the workforce is taking reasonable precautions, and another individual happens to see or overhear PII that the workforce member is using, the workforce member will not be held liable for that disclosure.

  Reasonable precautions include:

  - ✓ Keeping one's voice low while discussing information;
  - ✓ Moving to as private a location as possible while using information; and
  - ✓ Keeping PII in paper and electronic formats covered or otherwise inaccessible to those who do not have authorization or a legitimate need to know the information.

  Incidental disclosures are not considered Privacy Incidents and do not usually need to be reported. However, members of the workforce should use professional judgment in assessing the potential outcome(s) of an incidental disclosure and report any disclosures that may result in a fraudulent or criminal misuse of the information or have a negative impact on the Department of the Interior or its affiliated entities.

- *Accidental Disclosures*: Unintentional disclosures of PII that is maintained in Privacy Act systems of records and other instances that apply to the definition of PII as detailed in OMB Memorandum M-07-16 and that occur as a result of carelessness and/or failure to follow established policies and procedures, but without malicious or premeditated intent.

  All members of the workforce are required to acknowledge and report known and suspected accidental disclosures of PII immediately:

  - ✓ So that the situation can be investigated and damage minimized or averted; and
  - ✓ The circumstances that led to the disclosure can be avoided to prevent further similar disclosures.

  Accidental disclosures are considered Privacy Incidents and must be reported immediately to the BITSM, bureau Privacy Officer, and DOI-CIRC. Examples of accidental disclosures include, but are not limited to:

  - o Disclosure of PII to a person requesting the information without verifying the person's identity and authority first.
  - o Leaving PII materials unattended in a public area: unable to retrieve or find them after the fact.
  - o Disposing of intact PII documents or electronic media in regular waste receptacles. (e.g., without shredding hardcopy documents or appropriately sanitizing media.)
  - o Leaving a message that contains PII on an answering machine.

  Members of the workforce should assist in correcting or recovering from a disclosure ONLY if instructed to do so by the ITTF, or its assigned agents.

- *Intentional Disclosures:* Disclosures of PII that occur as a result of deliberate and/or pre-meditated disregard of

established policies and procedures, with or without malicious intent.

All members of the workforce are obligated to report any known and suspected intentional disclosures of PII immediately. Examples of intentional disclosures include, but are not limited to:

- Gaining access to PII by deliberately circumventing security measures, by using someone else's password, or by other fraudulent means;
- Disclosing PII to unauthorized persons;
- Disclosing PII with intent to harm others by, or to profit personally from, the disclosure; or
- Compiling and saving unencrypted PII on portable computers or computer media.

Intentional disclosures are Privacy Incidents and will result in disciplinary action and the application of sanctions by the Department, and may also result in personal liability, either in civil or criminal legal action.

When a Breach Occurs

When a breach occurs, the following 5 major actions are required (individual steps are explained in each of the sections that follow):

(a) Detection (See Section 3.5)
(b) Reporting – Requirements and Procedures (See Sections 3.6 and 3.7)
(c) Assessing (See Sections 3.9 to 3.14)
(d) Completing Mitigation and Notification as needed (See Section 3.15)
(e) Review of Lessons Learned (See Section 3.16)

3.5 Detection of a breach

A confirmed or suspected breach can be detected by various personnel and in the various organizations of the Department (refer to the breach incident reporting procedures in sections 3.7 and Appendix D of this document). The detection of a breach or an event which could result in a breach affecting information processing systems at DOI is the responsibility of Bureau and Office Information Technology Security and Privacy Programs (ITSPPs), bureau and office incident response teams, or whoever first discovers or receives information about a breach involving PII.

Bureau Information Technology Security Programs (BITSPs) and Information Reduction Teams (IRTs)[21] will follow existing procedures if they detect or suspect a breach, and notify the BITSM, Bureau/Office Privacy Officer and BITTF when reporting all privacy breach conditions.

Next, the BITSM, in consultation and coordination with the Bureau Privacy Officer and BITTF Lead, will notify the DOI-CIRC of the incident, monitor the evolving situation, and if appropriate, will then proceed according to a predefined set of notification parameters. While the BITTF Lead will oversee the notification process of individuals affected by the breach, the Bureau/Office, or other Department unit from which the information was acquired will be responsible for the costs and labor associated with notifying the affected persons.

Normally, DOI-CIRC and the Office of the Inspector General (OIG) receive the initial notice through their situational awareness monitoring capability (DOI-CIRC Portal and DOI Watch Office). When a breach occurs that has resulted or could result in a loss of privacy information, the following people must be notified:

- Supervisor of the party that detected the breach
- Bureau/Office IT Security Manager
- Bureau/Office Privacy Officer
- Bureau/Office Identity Theft Task Force

Disclosures by whistleblowers: Neither the Department, nor any of its workforce members, affiliated entities, or business associates shall be deemed to have violated the requirements of federal privacy regulations if the individual or entity:

- Reports immediately unlawful conduct or suspected unlawful conduct which creates and presents a substantial and specific danger to the public's health, safety or welfare; and

- Has a good faith belief that the Department or its workforce members, affiliated entities, or business associates have engaged in conduct which violates professional or clinical standards or Department rules or policies; or

- Discloses information to:

    - An agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the Department, or to an appropriate accreditation organization for the purpose of reporting the allegation of failure to meet professional standards;

[21] For a detailed description of the duties of the Information Reduction Teams, see OCIO Directive issued September 2007 and entitled "Departmental Strategy to Safeguard Personally Identifiable Information and Reduce the Collection and Uses of Social Security Numbers."

or misconduct by the Department, its employees or business associates; or

- An attorney retained by, or on behalf of, the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

3.6 Requirements for reporting breaches of PII

After a breach is detected through the steps noted above, it is imperative that a reporting of the breach take place prior to assessment of the incident. This Section of the Strategy provides guidance on the reporting requirements, which Section 3.7 provides information on the procedures for reporting. Assessment is addressed further starting with Section 3.9.

There are a number of existing requirements with which agencies must comply regarding breaches of PII. Pursuant to the Federal Information Security Management Act (FISMA), agencies must:

- Implement procedures for detecting, reporting and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done.
- Notify and consult with Federal information security incident center, law enforcement agencies, Inspectors General, an office designated by the President for any incident involving a national security system, any other agency or office in accordance with law or as directed by the President.
- Implement NIST guidance and standards.[22]

Agencies must also develop incident handling and response mechanisms that would enable them to respond in a manner protecting both its own information and help to protect the information of others who might be affected by the incident. To meet this requirement, Agencies must establish formal incident response mechanisms. To maximize effectiveness, incident handling and response must also include sharing information concerning common vulnerabilities and threats with those operating other systems in other agencies. All employees must be trained on how to prevent incidents and their roles and responsibilities regarding responding to incidents that may occur.

[22] The procedures agencies must currently use to implement the above FISMA requirements are found in two primary guidance documents: National Institute for Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide* and the concept of operations for the Federal security incident handling center located within the Department of Homeland Security, *i.e.*, United States Computer Emergency Readiness Team (US-CERT) (See 44 U.S.C. § 3546).

3.7 Breach Incident Reporting and Handling Procedures[23]

For breaches involving protected health information (PHI) or PII, all employees, contractors, volunteers, and official visitors, who are employed by or otherwise associated with the Department of the Interior's components and affiliated entities, are obligated to report any known or suspected violations or breaches of PII to their immediate supervisor, the BITSM, their Bureau/Office Privacy Officer and law enforcement if a data management device is lost or stolen.

In instances of a breach (both potential and confirmed) involving PII, the party that detects the breach must:

- Take immediate steps to secure the affected system. Follow your bureau's specific information security procedures.
- Report the breach immediately, along with your contact information, to your supervisor, your Bureau Information Technology Security Manage (BITSM), and the bureau or office Privacy Officer. (If a computer or other data management device is lost or stolen, the BITSM or their designee, in coordination with the bureau or office Privacy Officer, and in consultation with the individual reporting the incident, must ***immediately*** complete an incident report and submit it to DOI-CIRC- See Appendix A of this Strategy.)
- Include the date, time and location of the incident, the nature of the violation, the type of PII involved, other persons involved, any immediate harm known or observed, and immediate corrective actions already taken. (See Appendix A of this Strategy for copy of the "Missing IT Asset Impact Analysis Form.")

Once the party detecting the breach has notified his/her supervisor, Bureau/Office Privacy Officer and BITSM, the flowing procedures are to be followed:

- The BITSM must notify the DOI-CIRC of the breach incident.
- DOI-CIRC must then notify US- Computer Emergency Readiness Team (US-CERT) ***within one hour*** of detection or discovery of the breach where an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource or if there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred.[24]

[23] This strategy applies to employees, contractors and other personnel in public-private partnership in an operating system.

[24] Bureau/Office specific bank and financial notification procedures for breach incidents involving government-authorized credit cards pursuant to OMB Memorandum M-07-16 will be included with this Strategy as they evolve.

- The BITSM will notify the Bureau/Office Privacy Officer and the BITTF Lead.

- The BITTF Lead must notify the Department Privacy Officer of the breach incident and the Interior ITTF Lead. Depending on the severity of the incident the Senior Agency Official for Privacy will convene the Interior ITTF.

- The BITTF must recommend corrective action and sanctions to Bureau Managers who are responsible for implementing the recommendations

Based on the nature and level of severity of the violation, and any history or pattern of previous violations, disciplinary action will be taken up to and including dismissal, in accordance with applicable Laws and/or rules, regulations, and policies, as appropriate.

If, after investigation, the BITTF determines that notification of affected persons or mitigation is reasonably required, persons involved in the incident may be asked to assist with the notification process and/or in mitigating the harmful effects (see Section 4.0 of this Strategy, External Breach Notification).

3.8 Incident Response Checklist

After a breach is detected and reported, there are additional steps that must be followed. The "checklist" below provides an outline so that these critical steps can be completed successfully. The assessment process includes several key elements, specified in Sections 3.9 through 3.14 prior to the mitigation and external notification processes.

Upon notification of a breach incident, the BITTF will convene and determine appropriate responses. These activities will follow the steps outlined below. Further details on each step are provided in the sections below:

- ☐ Perform Initial Assessment of Incident
- ☐ Confirm Completion of Appropriate Internal Notifications
- ☐ Confirm Involvement of Appropriate Personnel
- ☐ Determine Exact Nature of Information Loss
- ☐ Analyze Information Loss to Determine Potential Impacts
- ☐ Determine Mitigation Plan of Action
- ☐ Determine External Notification Plan of Action (see Section 4.0 of this Strategy)
- ☐ Complete Mitigation and External Notification Activities (See Section 4.0 and Appendices B and C of this Strategy)
- ☐ Review Lessons Learned

3.9 Perform Initial Assessment of Incident

Based on a summary of the breach incident, an initial assessment of the incident will be completed by the relevant Bureau/ Office ITTF. This assessment will include an assessment of internal notifications that need to be completed. The assessment will also identify staff outside of the BITTF that will need to participate in incident response activities.

3.10 Confirm Completion of Appropriate Internal Notifications

The BITTF will confirm that the notifications identified during the initial assessment are completed. Note that these are notifications that are internal to the Department of the Interior and the Federal Government (e.g. DOI-CIRC, US-CERT, OMB), *not external notifications to affected individuals or the press.*

3.11 Confirm Involvement of Appropriate Personnel

The BITTF will confirm the participation and availability of personnel outside of the BITTF that will need to participate in incident response activities. This includes personnel from within the affected bureau or office and additional staff from the organizations represented on the BITTF.

3.12 Determine Exact Nature of the breach

The affected bureau or office will take the lead in documenting the exact nature of the information lost. This step includes the identification of the sensitivity of the information, whether Indian Trust Data is involved, the number of individuals impacted, etc. The "DOI Missing IT Asset Impact Analysis" form (see Appendix A) will be used to collect this information. This form and any other supporting documentation (*e.g.*, examples of documents that were lost) will be provided to the BITTF and when required the Interior ITTF.

3.13 Analyze PII Involved to Determine Potential Impact

Based on the information provided in the previous step, an analysis of the information lost and the potential impact will be conducted. Responsibility for the completion of this analysis will be determined by the BITTF based upon the specific nature of the incident.

This analysis must consider factors including:

- ✓ Was the loss intentional?
- ✓ Was the data the target?
- ✓ Was the PII in question, as defined under the Privacy Act, lost?
- ✓ Could loss result in Privacy Act harm/liability?
- ✓ How many individuals were affected?
- ✓ Are the identities of the affected individuals revealed or potentially known?

3.14 Determine Mitigation Plan of Action

Based upon the analysis performed in the previous step, the BITTF will determine appropriate actions to mitigate the impact of the incident. These actions may include:

- Whether or not notification is necessary.
- Analyze factors to take into account in determining whether or not to notify affected individuals.
- Provision of credit monitoring services to affected individuals.
- Establishment of a call center to assist affected individuals (see Appendix B for guidance regarding the establishment of call centers).

DOI will make good faith efforts to mitigate, to the extent practicable, any harmful effect that is known to have occurred as a result of a use or disclosure of PII and PHI information by DOI or its business associates in violation of DOI's policies and procedures or of the privacy regulations. The following factors will be evaluated to determine whether or how to mitigate any damages:

- Likelihood of damage may not be immediately known therefore re-assessment of the level of impact as defined by NIST may be necessary as more information becomes available:

    1. Low- the loss of confidentiality, integrity, or availability is expected to have a *limited* adverse affect on organizational operations, organizational assets or individuals.

    2. Moderate- the loss of confidentiality, integrity, or availability is expected to have a *serious* adverse affect on organizational operations, organizational assets or individuals.

    3. High- the loss of confidentiality, integrity, or availability is expected to have a *severe or catastrophic* adverse affect on organizational operations, organizational assets or individuals.

- The nature of the damage that occurred, if any;
- Likelihood of data being accessible;
- The amount of damage, if any;
- The PII that was used or disclosed;
- The reasons for the use or disclosure; and
- Whether the harm can be mitigated.

3.15 Complete Mitigation Plan of Action and External Notification

Following the assessment of the breach incident, the mitigation plan of action and external notification should be completed as determined appropriate by the BITTF based on the nature of the incident. Section 4.0 of this Strategy, "External Breach Notification," details the external breach notification policy for incidents involving PII and may be consulted for further information.

Note that the Director of Public Affairs, or designee, is responsible for directing all meetings and discussions with the news media and the public, in coordination with the BITTF and/or Interior ITTF. In the absence of Public Affairs representative, the responsibility reverts to the Deputy Secretary.

3.16 Review Lessons Learned

The final step in incident response activities is for the ITTF to perform an assessment of "lessons learned" and to consider whether modifications to the Privacy Loss Mitigation Strategy or incident handling procedures are warranted.

BITTF and ITTF should notify Bureau/Office Information Reduction Teams in cases where PII collections involved in an incident might be reduced.[25]

[25] See footnote 22 of the Strategy regarding the formation and duties of the information reduction teams.

4.0 External Breach Notification

Once the BITTF is notified that there is a breach of PII, persons affected by the breach will be notified by the Agency Head or senior-level personnel he/she may designate in writing without unreasonable delay, but no later than ten (10) business days after the determination is made.[26] When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring that any notification and corrective actions are taken.[27]

4.1 External Notification Determining Factors

The need for providing an external notification of a breach to impacted individuals should be assessed on a case by case basis. There are six elements which should be considered in determining if external notification is necessary:

1. Whether the breach notification is required;
2. Timeliness of the notification;
3. Source of the notification;
4. Contents of the notification;
5. Means of providing the notification; and
6. Who receives the notification: public outreach in response to a breach.

4.2 Whether Breach Notification is Required

In assessing whether breach notification is required, the following should be considered:

- Nature of the data elements breached- consider the elements of data in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals;

- Number of individuals affected- the magnitude of number of affected individuals may dictate the method(s) one chooses to provide notification, but should not be the determining factor for whether an agency ultimately should provide notification;

- Likelihood the information is accessible and useable- upon learning of a breach, agencies should assess the likelihood PII will be or has been used by unauthorized individuals. An increased risk the information will be used by unauthorized individuals may influence the agency's decision to provide notification. The

[26] Notification involving only a limited number of individuals (*e.g.*, under 50) may be also issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer or Senior Agency Official for Privacy.

[27] The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

assessment of risk of use should be guided by NIST standards and guidance;

- Likelihood the breach may lead to harm- possible harms associated with a breach, such as potential for blackmail, mental pain, emotional distress, disclosure of address information for victims of abuse, or secondary uses of information that can lead to fear or unwarranted exposure leading to humiliation or loss of self-esteem; use of certain information, such as social security numbers, for identity theft; and

- Ability of the Agency to mitigate the risk or harm- containing the breach, appropriate counter measures to prevent further damage, can limit associated harm of breach.

4.3 Timeliness of Notification

The relevant BITTFs must convene immediately once a breach is discovered to include PII. BITTFs must also evaluate whether notification can be made to affected individuals and which notification actions to take. BITTFs will "take any measures necessary [to] determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised."[28] Any decisions to delay notification should be made by the Secretary of the Interior or a senior-level individual he/she may designate in writing.[29]

4.4 Source of Notification

The Secretary or designee will issue an external notification of a breach involving PII. Notification involving only a limited number of individuals (*e.g.*, under 50) may also be issued jointly under the auspices of the Chief Information Officer and the Departmental Privacy Officer or Senior Agency Official for Privacy.[30]

4.5 Contents of Notification

Once a determination has been made by the BITTF that actual notification of a breach should be issued to the individuals of the breach, within ten (10) business days of that determination a notification should be issued with the following components:

- A general description of the incident;

- The Police Report number, if available;

- Instructions and necessary information for notifying the major credit agencies of suspected or potential identity theft; and

---

[28] See OMB Memorandum M-07-16, Attachment 3, pg. 16.
[29] *Id.*
[30] *Id.*

- The Bureau/Office or when applicable the Department's Privacy Office telephone numbers, including a Hotline number, and website information as appropriate.

4.6 Methods of Providing Notification

Means of notification to individuals impacted by a breach will depend on the number of individuals affected, what contact information is available for affected individuals, and the best form of communication so as not to unnecessarily alarm the public.[31] Examples of such forms of notification include:

- Telephone contact may be appropriate when circumstances dictate urgency and when a limited number of individuals are affected.

- First-Class Mail notice should be sent separately from any other mailing so that it is conspicuous. The front of the envelope should be labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed" and should be marked with the name of the Agency as the sender to reduce the likelihood the recipient thinks it is advertising mail.

- E-mail may be used when an individual has given consent to use e-mail as a primary means of communication with the agency and no known mailing address is available. E-mail may also be used in conjunction with postal mail if the circumstances of the breach warrant such an approach. E-mail notification should include links to the agency and www.usa.gov websites.

- Existing Government-wide Services such as USA Services, including toll-free number of 1-800-FedInfo and www.usa.gov.

- Newspapers or other public media outlets can be used as a form of notification. In such cases, toll-free call centers staffed by trained personnel will be established to handle inquiries from affected individuals and the public.

- Substitute Notices can be used in instances where the Agency does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of your agency's website and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free number where an individual can learn whether or not his or her personal information is included in the breach.

---

[31] *Id.*

- Accommodations should be made for individuals who may be visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type posting on the agency website.

4.7 Notification of Third Parties

Notification of Third Parties including the Media will require careful planning and execution so as not to unnecessarily alarm the public.[32] Based upon the analysis described in Section 4.1, the BITTF (or ITTF in certain instances) will determine appropriate notification to parties external to the Department of the Interior or the Federal Government. This determination must also identify how and when the notification will be accomplished. External parties to be notified may include:

- Notification to affected individuals (see Appendix C for sample notification letters);

- Notification to the general public and the news media in a format to be determined based on the type and scope of the breach. (See Sample Press Release in Appendix C.)

When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification has been developed. Notification may be delayed upon the request of law enforcement or national security agencies as described above in Section 2.3. To the extent possible, when necessary prompt public media disclosure is generally preferable because delayed notification may erode public trust.

Any web posting about breach and notification should be done in a clearly identifiable location on the home page of the Agency website as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The post should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach.

Public and Private Sector Agencies may need to be notified on a need to know basis, particularly those that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach.

Congressional inquiries may be made and the Agency should be prepared to respond to these and inquires from other governmental agencies such as the Government Accountability Office.

[32] See OMB M-07-16, Attachment 3(A)(4).

Appendix A

DOI Missing IT Asset Impact Analysis Form

INSTRUCTIONS	Use Missing IT Asset Impact Analysis per DOI Incident Response policy. Complete all required information. Attach supporting evidence such as logs, screenshots, files and reports.

ASSESSOR INFORMATION

Name: _____ Ext____ Signature:

_____ Date: _____

I. INFORMATION ABOUT ASSET

❑ Laptop ❑ Desktop ❑ Blackberry ❑ ID Card ❑ Other (describe)

_____

Brand/ Model: _____ Serial Number: -

_____

Asset Tag Number: _____

II. ASSET LOSS INFORMATION

Person Asset Assigned To: _____ Date/Time Reported Missing:

_____

Asset Location: _____ Date/Time Last in Possession:

_____

Brief Description of How Loss Occurred:

_____

_____

_____

III. DESCRIPTION (IN DETAIL) OF PHYSICAL AND TECHNICAL PROTECTIONS ON ASSET:

IV. IMPACT ANALYSIS							
INFORMATION TYPE & SOURCE [33]	POTENTIAL IMPACT [34]			SENSITIVE DATA INVOLVED		WAS THE INFORMATION ENCRYPTED? (YES/NO)	SCOPING/MITIGATING FACTORS (IN ADDITION TO ANY OTHER FACTORS, INCLUDE: A DESCRIPTION OF THE PRODUCT USED TO ENCRYPT THE DATA; IF THE ENTIRE DRIVE IN QUESTION WAS ENCRYPTED OR JUST THE FILE; IF ONLY THE FILE WAS ENCRYPTED, IS THERE A LIKELIHOOD OF DATA REMNANTS ELSEWHERE ON THE DRIVE; AND INDICATE IF THE ENCRYPTION WAS COMPLIANT WITH THE MOST CURRENT VERSION OF NIST FIPS PUB 140-XXX.)
	LO	MED	HI	PII [35]	IITD [36]		

INFORMATION TYPE [37]	PII AND/OR IITD DESCRIPTION	AFFECTED INDIVIDUALS [38]

V. ADDITIONAL PROTECTIONS/ACTIONS TAKEN RESULTING FROM IMPACT ANALYSIS:

REVIEWERS INFORMATION

Name: _____ Ext____ Signature:

_____ Date: _____

VI. REPORTING ☐ OIG ☐ DOI CIRC ☐ DHS US-Cert ☐ Bureau CIRC/CERT ☐ LOCAL POLICE

VII. ROUTING ☐ SAOP ☐ CIO ☐ CISO ☐ OIG ☐ Solicitor ☐ DHS US-Cert

[33] Information Type from NIST 800-60 (in addition to the source of information, also indicate information ownership)

[34] Potential impact from NIST 800-60 as modified using scoping/mitigating factors

[35] Check if the data contained PII.

[36] Check if the data contained IITD (if not checked but Trust Data was involved, address in Scoping section).

[37] Complete one row for each Information type containing PII.

[38] Provide an estimate of the number of individuals whose data is compromised.

Appendix B

General Guidance for the Establishment of a Call Center in the Event of a Privacy Act Breach

In the event of a significant privacy breach of Personally Identifiable Information (PII) the following guidance is provided as the BITTF or Interior ITTF considers whether to establish a call center to handle inquiries related to the incident. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the spillage and possible actions they may want to take to lessen the incident's impact on their personal lives (i.e., identity theft, etc.).

The decision to establish a call center should be based on several considerations:

- If a bureau has a privacy breach that does not extend outside the organization (i.e., those affected by the breach are known and can be contacted), then establishment of a call center would not normally be necessary.

- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted, establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach.

- Each situation will be unique and the decision to establish a call center must be based on the individual circumstances. The main concern should be the sharing of information with those affected and how they may obtain assistance.

- Once the decision is made to establish a call center there are several follow-up options:

    - Contact the National Business Center (NBC) to obtain a toll-free number. This option is most likely the least expensive, since the impacted bureau will be providing its own personnel to staff the call center.

    - Contact the General Services Administration's (GSA) USA Services Group to establish a call center supported and manned by GSA personnel. A statement of work (SOW) will be required and the call center can be up and running usually within 72 hours. SOW requirements can be found at http://www.usaservices.gov under FirstContact. A generic SOW is provided there. A thorough description of the incident and set of frequently asked questions will also be required for GSA personnel to refer to when fielding questions. GSA POCs are: Ms. Teresa Nasif at 202-501-1794 and Mr. Bob Corey, Contracting Officer, at 202-501-1797.

Suggested items to consider based on the nature of the breach would include but are not limited to:

- Use of existing bureau personnel to man the call center and the number of individuals required.
- Training of call center operators.
- Pre-staged frequently asked questions (FAQs). Below are questions used during the Veteran's Administrations privacy breach in May 2006. These could be used as a starting point and tailored to meet the requirements of a specific breach.
- Ability to adjust manning in response to call volume.
- Daily hours of operation.
- Cost of service.
- Logging calls.
- Bureau and Department reporting requirements.
- Advertising call center number(s) and making breach information readily available to those affected (i.e., on bureau's and other appropriate websites, mass emailing(s) to those affected, news media, etc.).
- Department periodic check of call center quality of customer service.
- Criteria to disestablish call center.
- Ensure training procedures are in place to prevent additional inadvertent disclosure of PII or sensitive agency information resulting from legitimate or illegitimate deliberate calls attempting to exploit social engineering weaknesses to gain additional unauthorized access to or disclosure of information.

Sample Call Center Frequently Asked Questions:

1. *How can I tell if my information was compromised?*

   At this point there is no evidence that any missing data has been used illegally. However, the Bureau of _____ is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions. If you notice unusual or

suspicious activity, you should report it immediately to the financial institution involved.

2. *What is the earliest date at which suspicious activity might have occurred due to this data breach?*

   The information was stolen from an employee of the Bureau of _____ during the month of _____, 20XX. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity during the month of _____.

3. *I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?*

   The Department of _____ strongly recommends that individuals closely monitor their financial statements and visit the Department of _____ special website at www._____.gov.

4. *Should I reach out to my financial institutions or will the Department of _____ do this for me?*

   The Department of _____ does not believe that it is necessary to cancel credit cards and bank accounts, unless you detect suspicious activity. However, you should contact your financial institutions (e.g., bank or financial lenders, credit card companies, the Social Security Administration, etc.) to notify them that your PII may have been lost, stolen or obtained by an unauthorized third-party and have a "fraud alert" placed on your accounts/files.

5. *Where should I report suspicious or unusual activity?*

   The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

   - Contact the fraud department of one of the three major credit bureaus:

     Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.

     Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, Texas 75013.

     TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

   - Close any accounts that have been tampered with or opened fraudulently.

- File a police report with your local police or the police in the community where the identity theft took place.

- File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline by telephone: 1-877-438-4338, online at www.consumer.gov/idtheft, or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

6. *I know the Department of _____ maintains my health records electronically. Was this information also compromised?*

   No electronic medical records were compromised. The data lost is primarily limited to an individual's name, date of birth, social security number, in some cases their spouse's information, as well as some disability ratings. However, this information could still be of potential use to identity thieves and we recommend that all individuals be extra vigilant in monitoring for signs of potential identity theft or misuse of this information.

7. *What is the Department of _____ doing to ensure that this does not happen again?*

   The Department of _____ is working with the President's Identity Theft Task Force, the Department of Justice and the Federal Trade Commission to investigate this data breach and to develop safeguards against similar incidents. The Department of _____ has directed all employees to complete the "DOI Cyber Security Awareness Training Course" and complete the separate "DOI Employee Privacy Awareness Course" by _____, 20XX. In addition, the Department of _____ will immediately be conducting an inventory and review of all current positions requiring access to sensitive data and require all employees requiring access to sensitive data to undergo an updated National Agency Check and Inquiries (NACI) and/or a Minimum Background Investigation (MBI) depending on the level of access required by the responsibilities associated with their position. Appropriate law enforcement agencies, including the Federal Bureau of Investigation and the Inspector General of the Department of _____, have launched full-scale investigations into this matter.

8. *Where can I get further, up-to-date information?*

   The Department of _____ has set up a special website and a toll-free telephone number for employees which features up-to-date news and information. Please visit www._____.gov or call 1-800-XXX-XXXX.

9. *Does the electronic data theft affect only _____?*

It potentially affects all employees hired since _____, which is when automated records management began and regular input of information commenced.

We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.

Appendix C

Sample Written Notification

SAMPLE LETTER 1

Data Acquired: Credit Card Number or Financial Account Number Only
(NOTE: DO NOT insert actual credit card or financial account numbers!)

Dear :

We are writing to you because of a recent security incident at [name of responsible bureau or office]. [Describe what happened in general terms, what type of Personally Identifiable Information was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you immediately contact [credit card or financial account issuer] at [phone number] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask [name of account issuer] to give you a PIN or password. This will help control access to the account.

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at http://www.consumer.gov/idtheft.

If there is anything [name of responsible bureau or office] can do to assist you, please call [toll-free phone number].

[Closing]

SAMPLE LETTER 2

Data Acquired: Driver's License or ID Card Number
(NOTE: DO NOT insert actual credit card or financial account numbers!)

Dear :

We are writing to you because of a recent security incident at [name of responsible bureau or office]. [Describe what happened in general terms, what kind of Personally Identifiable Information was involved, and what you are doing in response.]

Since your Driver's License number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free DMV Fraud Hotline at [Insert Hotline Number] for additional information.

To further protect yourself, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at a number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, carefully review them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for PII, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at http://www.consumer.gov/idtheft. If there is anything [name of responsible bureau or office] can do to assist you, please call [toll-free phone number].

[Closing]

SAMPLE LETTER 3

Data Acquired: Social Security Number
(NOTE: DO NOT insert actual Social Security Number!)

Dear :

We are writing to you because of a recent security incident at [*name of responsible bureau or office*]. [*Describe what happened in general terms, what kind of Personally Identifiable Information was involved, and what you are doing in response.*]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files (credit card companies, personal banking institutions, Social Security Administration, etc.). A fraud alert lets creditors know to contact you before opening new accounts. You can contact any one of the three credit reporting agencies at a number below to have a fraud alert placed on your account (you may be asked to contact other financial institutions separately). This will allow you to place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

When you receive your credit reports, look them over carefully for accounts you did not open. Also, look for inquiries from creditors that you did not initiate. In addition, look for personally identifiable information, such as home addresses and Social Security numbers that are not accurate.

If you see anything you do not understand, contact the credit reporting agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Alternatively, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Contact one of the credit reporting agencies above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at http://www.consumer.gov/idtheft. If you need further assistance, please contact [*name and telephone number of responsible bureau or office*].

[Closing]

SAMPLE NEWS RELEASE

Data Acquired: Social Security Number

Information on Departmental Security Issue

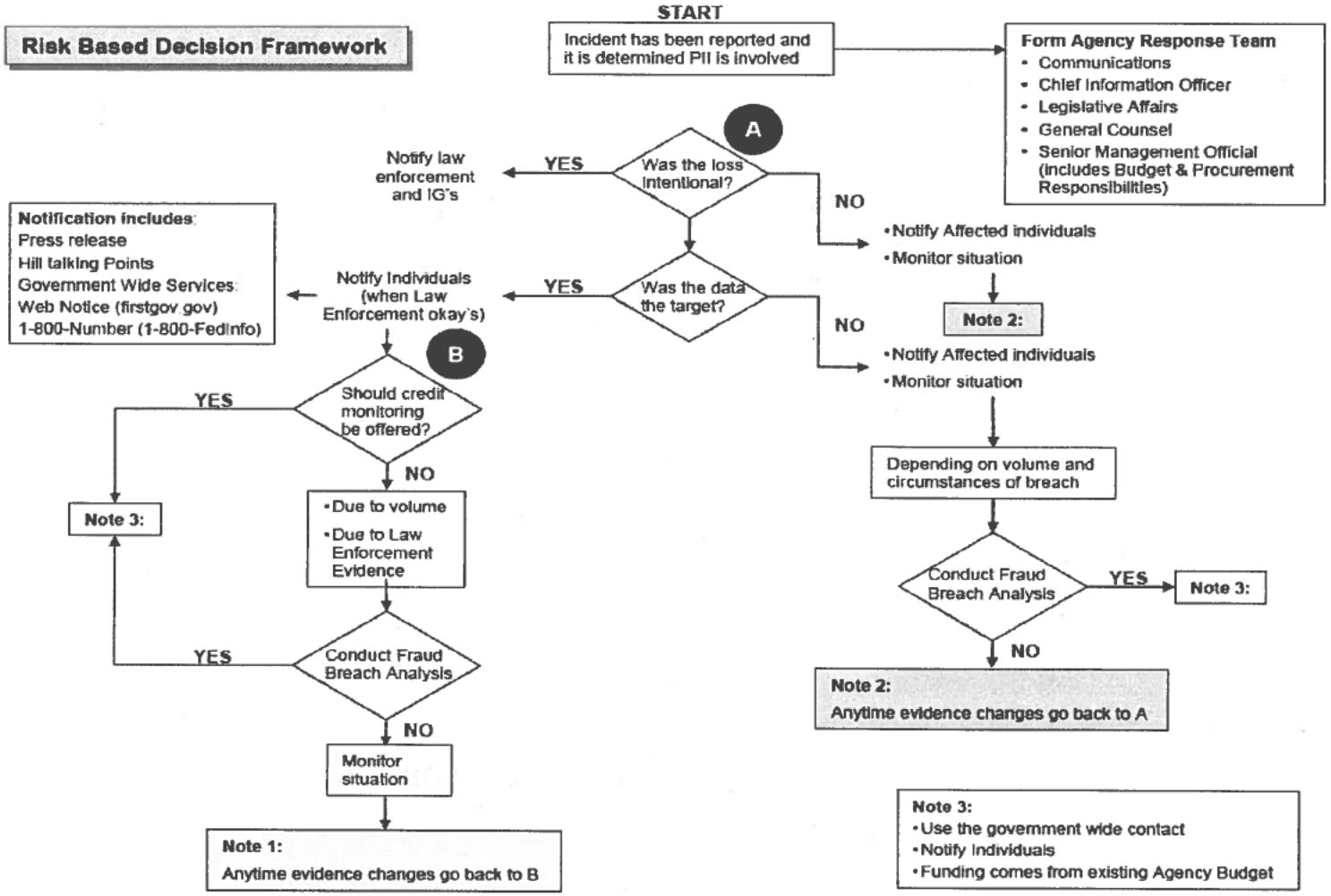
Media Inquiries: (202) _____

In May 2006, a laptop computer and hard drive containing sensitive data was stolen from a Department of _____ employee's home. The equipment was recovered and the FBI concluded that no personally identifiable information was accessed or compromised. Even before the equipment was recovered, the Department of _____undertook numerous actions to ensure the safety and security of information.

Since the incident, all Department of _____ employees have received training in the proper handling of sensitive information. Laptop computers throughout the department have previously had reliable data encryption programs installed and updated. Department of _____ Secretary _____ is committed to making the department the gold standard for all of government in the area of information security. " Department of _____ remains unwavering in its resolve to become the leader in protecting personal information, training and educating our employees in best practices, and establishing a culture that always puts the safekeeping of employees' personal information first," the Secretary said

Appendix D

Bureau/Office Identity Theft Task Force Strategy Flowchart



Appendix E

Definitions

Access: The ability or opportunity to gain knowledge of personally identifiable information.

Breach: The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to personally identifiable information in usable form, whether physical or electronic. A breach would not occur if, for example, the information was properly encrypted within a mobile computing device because the information would be unusable.

Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to a specific individual.

Privacy: Freedom of an individual from intrusion or observation; the right to maintain sole control over PII; and the expectation that others will respect the individual's rights.

Protected Health Information (PHI): individually identifiable health information (IIHI) that is maintained or transmitted in any form, including oral communications that is created or received by a health care provider, relates to the past, present or future physical or mental condition of an individual; provision of health care to an individual; or payment for that health care; and identifies or could be used to identify the individual.

Professional Need to Know: Specific and limited information necessary to complete assigned work, in the case of performing official business.

Security: Administrative, physical and technical safeguards, used to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration or destruction, to maintain the integrity of the information.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Mitigation: To make less severe, to partially remove, or to correct, so that harmful effects of an incident are reduced or eliminated.

Violation: Infraction of a law; going against established rules.

Examples of Violations

1. Misuse of computer access passwords (i.e., sharing or posting passwords, unauthorized use of others' accounts, allowing use of accounts by others, etc.)

2. Attempting to bypass or exploit physical or technical information security measures.

3. Accessing PII outside of your "Professional Need To Know", either for personal curiosity or as a "favor" for someone else.

4. Storing unencrypted PHI or PII on removable/portable computer media/devices, laptops, remote workstations, (disks, CD's, tapes, keys, etc.)

5. Unauthorized publication of PII in any medium.

6. Selling PII or inappropriately giving such information to the news media or other unauthorized recipients.

7. Unauthorized disclosure of PII to persons without a "Need to Know" either deliberately or accidentally (i.e., discussing PII in public places, leaving documents containing PII unattended in public places, posting PII on unsecured web-sites, sending PHI in emails outside of DOI systems, "misplacing" or otherwise losing unencrypted PHI or PII stored on removable computer media, etc.).

Department of the Interior
Departmental Manual

Effective Date:
Series: Information Resources Management
Part 375: IRM Program Management
Chapter 19: Information Security Program

Originating Office: Office of the Chief Information Officer

375 DM 19

19.1 **Purpose.** This chapter establishes the Department's information security program.

19.2 **Definitions.** Information security terms utilized in this chapter are defined in the National Institute of Standards and Technology (NIST) Internal Review 7298, *Glossary of Key Information Security Terms.*

19.3 **Scope.** This chapter applies to all employees and other users of Department of the Interior (DOI) information systems.

19.4 **Authorities.** Authorities for this chapter are listed in Appendix A. This chapter will be updated as necessary, such as when new laws concerning information security are enacted by Congress and/or new guidance is issued by the Office of Management and Budget (OMB) or NIST.

19.5 **Roles and Responsibilities of Department Personnel.** The roles and responsibilities of Department personnel with respect to information security are as follows:

A. Chief Information Officer (CIO). The CIO is the DOI Information Technology Risk Executive and is responsible for:

(1) Ensuring DOI information system risk management processes are linked to DOI mission risk management processes at the Department level; and information system risks are viewed from an agency-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions.

(2) Designating the following Information Technology program officials:

(a) Chief Information Security Officer (CISO)

(b) Authorizing Officials (AOs) - (must be designated in writing)

(3) Establishing department-wide information security policy, standards, and guidance; and overseeing implementation to ensure compliance for all information and information systems, as required by FISMA and 112 DM 24.

B. Heads of Bureaus and Offices. The Heads of Bureaus and Offices are responsible or ensuring compliance with applicable Federal laws, rules, regulations, policies, standards and procedures including those issued by OMB, NIST and the Department for their mission/business operations, practices, information and information systems.

C. Chief Information Security Officer (CISO). Responsible as the Senior Agency Information Security Officer (SAISO) for developing and maintaining an agency-wide information security program, the CISO is also responsible for carrying out the CIO's information security responsibilities under Federal law and heading an office with the mission and resources to manage the overall Information Security Program

D. Employees and Volunteers. Responsible for complying with applicable Federal laws, rules, regulations, policies, standards and procedures including those issued by OMB, NIST and the Department to include, but not limited to, the following:

(1) Properly using and protecting agency data, information and information systems ensuring their use is only for the execution of official duties or authorized purposes.

(2) Promptly reporting potential security incidents and breaches.

(3) Adhering to established Rules of Behavior.

(4) Completing required training.

19.6 **Applicable Standards and Guidelines**

A. Information Security Standards and Guidelines Issued by the OCIO. The OCIO shall issue the following information security standards and guidelines:

(1) Information security standards based on the NIST information security control standards in the current version of Special Publication (SP) 800-53, that pertain to NIST defined security categories or "control families" listed in the table in Appendix B.

(2) Information security standards specific to the needs of DOI.

(3) Information security guidelines governing the implementation of the standards referenced in sections 1 and 2 above for all IT infrastructure across the Department including all Bureaus, Offices and subordinate organizations.

(4) Security Technical Implementation Guides (STIGs) governing the technical implementation of the security standards referenced above.

B. Information Security Guidelines and Implementation Plans Issued by Bureaus and Offices. Bureaus and Offices are responsible for issuing the following information security guidelines and implementation plans:

(1) System Owners shall issue detailed information security plans consistent with the OCIO standards and guidelines defined above that must be approved by the Authorizing Official (AO).

(2) Assistant Directors for Information Resources shall issue information security guidelines that define how information security standards should be implemented across a Bureau or Office for mission applications. These guidelines may provide additional security details for a particular Bureau or Office and its mission IT systems, but may not contradict existing OCIO standards or guidelines.

C. Risk Management Framework.

(1) The OCIO will issue an Information Security Risk Management Framework (RMF) consistent with all relevant NIST standards.

(2) The RMF will establish the Department's strategy to mitigate information security risks associated with the operation and use of information systems and the implementation requirements of this strategy across the Department. Any residual information security risks will be explicitly accepted by the AO as part of the Assessment and Authorization (A&A) process for all Major Applications (MA) and General Support Systems (GSS).

(3) The NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* identifies additional roles and responsibilities required by the RMF.

The standards, guidelines, and implementation plans referenced above comprise the documentation necessary to effectively establish the information security program of the Department.

19.7 **Compliance with Standards and Guidelines**. The Office of the Chief Information Officer (OCIO) will issue information security standards and guidelines in support of this chapter and work with Human Resources personnel, contracting officers and any other personnel needed to ensure compliance with such standards and guidelines throughout the Department. Bureaus and Offices will issue guidelines and implementation plans, consistent with the OCIO standards and guidelines, and ensure compliance within their respective organizations of the OCIO standards and guidelines, as well as the Bureau and Office guidelines and implementation plans.

19.8 **National Security Systems and Sensitive Compartmented Information (SCI) Systems**

A. The Chief of National Security Programs within the Office of Law Enforcement and Security is responsible for obtaining accreditation of all national security systems processing classified information.

B. Systems within the Department that process Sensitive Compartmented Information (SCI) must meet the same security standards as systems that process controlled unclassified information.

C. In addition to the standards referenced in paragraph19.8 B., systems processing collateral (non-SCI) national security information must comply with security policy established by the Committee on National Security Systems (CNSS).

D. In addition to the standards referenced in paragraph 19.8 B., systems processing SCI must comply with security policy established by the Director of National Intelligence (DNI) in Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation.*

E. Bureaus and Offices shall comply with DOI policies and directives regarding national security information and industrial security programs, ICD 503 and CNSS policies to manage the security of their National Security Systems and use NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, to identify National Security Systems.

Appendix A: Relevant Authorities

Applicable Laws. A number of laws, policy guidelines, regulations and guidance directives mandate protection of Federal computers, information, and related resources. Applicable laws passed by Congress include:

Authority	Description
Federal Records Act of 1950, 44 U.S.C. §§21, 29, 31 and 33	Establishes the framework used by Federal agencies for their Records Management programs.
The Freedom of Information Act (FOIA) of 1966, 5 U.S.C. § 552	This law requires that Federal information be made available to the public except under certain specified conditions.
The Privacy Act of 1974, 5 U.S.C. § 552a	This law imposes collection, maintenance, use, safeguard, and disposal requirements for Executive Branch offices maintaining information on individuals in a "system of records."
Federal Managers Financial Integrity Act of 1982 (FMFIA), 31 U.S.C. § 3512	This law mandates that Federal agencies establish and maintain an internal control program to safeguard data processing resources, assure their accuracy and reliability, and protect the integrity of information resident on such systems.
Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030	This law provides for the punishment of individuals who access Federal computer resources without authorization, attempt to exceed access privileges, abuse government resources, and/or conduct fraud on government computers.
Government Performance and Results Act (GPRA) of 1993, 31 U.S.C. § 1101	This law establishes policies for managing agency performance of mission, including performance of its practices.
Paperwork Reduction Act of 1995, Revised, 44 U.S.C. §§ 3501-3520	This law provides for the administration and management of computer resources.
Clinger-Cohen Act – Information Technology Management Reform Act of 1996, 40 U.S.C. § 1401 et seq.	This law improves the acquisition, use, and disposal of Information Technology (IT) by the Federal government.
Federal Financial Management Improvement Act (FFMIA) of 1996, 31 U.S.C. § 3111	This law mandates Federal agencies to implement and maintain financial management systems that comply substantially with Federal systems requirements, Federal accounting standards, and the U.S. Government Standard General Ledger (SGL). FFMIA also requires GAO to report annually on the implementation of the act.

Authority	Description
National Information Infrastructure Protection Act of 1996, 18 U.S.C. § 1030	This law provides for the protection of computer resources.
Government Paperwork Elimination Act (GPEA) of 1998, 44 U.S.C. § 3504	This law provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information, the option of doing so electronically when practicable as a substitute for paper and to use electronic authentication methods to verify the identity of the sender and the integrity of electronic content.
E-Government Act of 2002, 44 U.S.C. § 101	This law enhances the management and promotion of electronic government services and processes by establishing a broad framework of measures requiring technology to enhance citizen access to government information services.
Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541	FISMA requires Federal agencies to establish agency-wide risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.

Executive Orders. The following are Executive Orders that provide details related to information security for Federal Agencies.

Executive Order 10450, Security Requirements for Government Employees, April 1953	This order establishes that the interests of national security require all government employees be trustworthy, of good character, and loyal to the United States.
Executive Order 13011, Federal Information Technology, July 1996	This order establishes policy for the head of each agency to effectively use information technology to improve mission performance and service to the public.
Executive Order 13103, Computer Software Piracy, September 1998	This order establishes policy that each executive agency shall work diligently to prevent and combat software piracy in order to give effect to copyrights associated with computer software.
Presidential Decision Directive 63: Critical Infrastructure Protection, May 1998	This directive requires that the United States take all necessary measures to swiftly eliminate

	any significant vulnerability to both physical and cyber attacks on critical infrastructures, including our cyber systems.
Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001	This order establishes policy that ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such information systems.

Executive Branch Policy. The policies listed below are established through directives published by the Office of Management and Budget (OMB) based on the applicable laws passed by Congress

OMB Circular	Description
A-11, Section 53, Information Technology and E-Government	This directive specifies the identification of security and privacy safeguards for managing sensitive information.
A-123, Management Accountability and Control, as revised December 21, 2004	This directive specifies the policies and standards for establishing, assessing, correcting, and reporting on management controls in Federal agencies.
A-127, Financial Management Systems, as revised by Transmittal Memorandum Number 3, December 1, 2004	This directive prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems.
A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals	This directive prescribes policy to agencies for the implementation of the Privacy Act and reporting requirements related to the management of personally identifiable information (PII).
A-130, Appendix III, Security of Federal Automated Information Resources, as revised by Transmittal Memorandum Number 4, November 28, 2000	This directive stipulates that each agency shall implement a comprehensive automated information security program. The appendix establishes basic managerial and procedural controls that shall be included in Federal automated information systems.

Appendix B: NIST Defined Security Control Standards

IDENTIFIER	SECURITY CONTROL STANDARD	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Federal Network Security
Federal Interagency Technical Reference Architectures

Domain Name System (DNS) Security Reference Architecture

Version 1.0

6/21/2011

Department of Homeland Security
National Cyber Security Division
Federal Network Security
Network & Infrastructure Security

Revision History

Date	Version	Description	Approved By
June 30, 2011	1.0	Final Version 1.0	Roberta G. Stempfley

Acknowledgements

This document is the product of a multi-agency collaborative initiative to provide guidance for the successful and secure implementation of Domain Name System (DNS) at Federal civilian agencies. Participants from several agencies have graciously volunteered their expertise; this document would not be possible without their selfless contributions.

Architecture Participants

Name	Agency
Paula Bailey	Department of Agriculture
Brian Kipper	Department of Homeland Security
Carl Beaudry	Department of Homeland Security
Earl Crane	Department of Homeland Security
Jim Rather	Department of Homeland Security
Richard Hudson	Department of Homeland Security
Robert Moore	Department of Homeland Security
Bill Lakner	Department of Labor
Ranny Reynolds	Department of the Treasury
James Boissonnault	Department of the Treasury (FMS)
Nnake Nweke	Federal Communications Commission
Peter Batista	Federal Communications Commission
Peter Cho	Federal Deposit Insurance Corporation
George Cartron	General Services Agency
Cathy Robertson	Internal Revenue Service
Timothy Morizot	Internal Revenue Service
Walter Lamar	National Institute of Health
Robert Toense	National Institute of Standards and Technology
Scott Rose	National Institute of Standards and Technology
Chi Kang	National Oceanic and Atmospheric Administration
Erwin Mascardo	National Oceanic and Atmospheric Administration
Sameka Prather	National Oceanic and Atmospheric Administration
Casey Deccio	Sandia National Laboratory
Donald Rudder	Tennessee Valley Authority
Brion Leary	U.S. Postal Service

Architecture Document Team Members

Name	Organization
Marilyn Rose	Department of Homeland Security (Project Leader)
Sean Donelan	Department of Homeland Security
Oscar Ahumada	Department of Homeland Security
Robert Moore	Touchstone Consulting Group
Eric Pratsch	Touchstone Consulting Group

Table of Contents

1 PURPOSE AND SCOPE 1

2 DNS ARCHITECTURAL COMPONENTS 2

1 2
2.1 NAME SERVER FUNCTIONAL TYPES 2
2.1.1 Authoritative Name Servers 2
2.1.2 Recursive Caching Name Server 2
2.2 NAME SERVER AUTHORITY 2
2.2.1 Primary Name Server 2
2.2.2 Secondary Name Server 2
2.3 NAME SERVER EXPOSURE 3
2.3.1 Public-Facing Name Server 3
2.3.2 Private Name Server 3

3 SECURITY PATTERNS 4

3.1 AUTHORITATIVE SERVER REQUIREMENTS 4
3.2 RECURSIVE CACHING SERVER REQUIREMENTS 5

4 SYSTEMIC THREATS & MITIGATIONS 7

5 DNS SECURITY CONFIGURATION 8

5.1 EXTERNAL AUTHORITATIVE SERVERS 8
5.2 RECURSIVE CACHING SERVERS 9
5.3 INTERNAL AUTHORITATIVE DNS SERVERS 10

6 IMPLEMENTATION CONSIDERATIONS 11

6.1 REMOTE VPN CLIENTS 11
6.2 DNS AND SECURITY POLICY 11
6.3 DNS OUTSOURCING 11
6.4 DNSSEC SIGNING 12
6.5 DNSSEC VALIDATION 13

APPENDIX A: ACRONYMS – COMMON ABBREVIATIONS 15

APPENDIX B: GLOSSARY – COMMON TERMS AND DEFINITIONS 17

APPENDIX C: SELECTED EXISTING GUIDANCE 20

LEGISLATION 20
POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA 20
STANDARDS 20
GUIDANCE 21

Index of Figures

FIGURE 1: DNS INFRASTRUCTURE MODEL 4

Index of Tables

TABLE 1: DNS THREATS 7
TABLE 2: CONFIGURATION SUMMARY OF EXTERNAL AUTHORITATIVE SERVERS 8
TABLE 3: CONFIGURATION SUMMARY OF RECURSIVE CACHING SERVERS 9
TABLE 4: CONFIGURATION SUMMARY OF INTERNAL AUTHORITATIVE SERVERS 10
TABLE 5: IMPLEMENTING DNSSEC SIGNING 12
TABLE 6: IMPLEMENTING DNSSEC VALIDATION 13

1 Purpose and Scope

The overall purpose of the DNS Security Reference Architecture is to optimize and standardize the DNS currently in use by the Federal civilian government, and to improve the Federal government's security posture by reducing the threats against the DNS at Federal civilian agencies. This is not mandatory implementation guidance and will supplement - not repeat or replace - existing policies and standards. The document helps agencies comply with relevant Federal policies and offers best practices, which may be customized to unique Federal civilian agency requirements.

This document is a reference that provides insight and guidance for agencies implementing DNS and striving to comply with OMB M-08-23 *Securing the Federal Government's Domain Name System Infrastructure*. This document is descriptive in nature, recognizing that many organizations face unique challenges that do not lend themselves to a "one size fits all" solution. Unlike a Target Architecture, a Reference Architecture does not mandate specific solutions, but rather identifies a range of workable modular solutions.

The intent is to enable agencies to leverage existing capabilities and technologies when implementing DNS in evolving Enterprise Architectures and to achieve compliance with the National Strategy for Trusted Identities in Cyberspace (NSTIC) in the context of their respective missions, programs, and initiatives. NSTIC calls for the development of interoperable technology standards and policies — an "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. DNSSEC is a critical enabling technology for NSTIC.

This document is intended for use by Federal civilian agencies. The information in this document is based upon collaboration with multiple agencies, the definitions and requirements in the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) guidance and standards, TIC Reference Architecture v2, and Office of Management and Budget (OMB) Memoranda.

2 DNS Architectural Components

DNS is a globally distributed database accessed using a simple query/response protocol. The DNS protocol resolves human readable domain names (e.g., "www.agency.gov") to an Internet Protocol (IP) address and is often the first step in any network communication. An agency's DNS is a key component of its network infrastructure. Therefore it is vital that the DNS infrastructure is responsive, robust, and secure so that it can meet its two primary business purposes: (1) allow agency personnel to reach the Internet; and (2) allow the general public to reach the agency's public-facing web services.

2.1 Name Server Functional Types

For the purposes of this Architecture, DNS components can be divided into two broad functional categories: components that maintain and distribute domain names for clients (Authoritative Name Servers), and components that request domain names from servers (Recursive Caching Name Servers).

2.1.1 Authoritative Name Servers

Authoritative servers maintain a portion of the global DNS database for an enterprise (referred to as its **zone**, as an example, 'agency.gov'). The authoritative servers for the respective zones are able to provide any resolution within its portion of the name space (e.g. *.agency.gov) or issue an error message such as NXDOMAIN (not able to resolve the requested name to an IP address).

2.1.2 Recursive Caching Name Server

A **recursive caching server** (or "caching resolver server") performs DNS resolution on behalf of clients ("stub" clients without the ability to do a full DNS query.) It then stores the responses in a cache for the benefit of all the stub clients it services.

2.2 Name Server Authority

Authoritative servers are further divided into two categories: **primary** (or "master") and **secondary** (or "slave").

2.2.1 Primary Name Server

A **primary** name server loads its information from a locally maintained file or database.

2.2.2 Secondary Name Server

A secondary name server is an authoritative name server which obtains the zone information that it serves from a primary name server instead of a locally maintained database. This is usually accomplished within the DNS protocol by means of a **zone transfer**. A zone transfer is a special type of DNS query and response that transfers the contents of a zone database in a single

transaction and is often done over TCP rather than UDP (as traditional query/response transactions). Some DNS implementations do not use zone transfers to replicate zone information; instead these use some other data replication services to perform a functionally equivalent task. Regardless of what protocol is used, a name server is secondary if it obtains its zone information from another server.

2.3 Name Server Exposure

Authoritative servers are classified according to the following exposure levels: public-facing or private.

2.3.1 Public-Facing Name Server

An authoritative name server is "public-facing" if it responds to DNS queries from an external network. It is usually located in an agency's DMZ but may reside elsewhere. An authoritative server's zone information includes the addresses of all externally facing services (e.g. web, mail, etc.). Public-facing name servers should always be authoritative because public-facing recursive caching servers are more vulnerable to cache poisoning attacks and can be used as reflectors for distributed denial of service (DDoS) attacks.

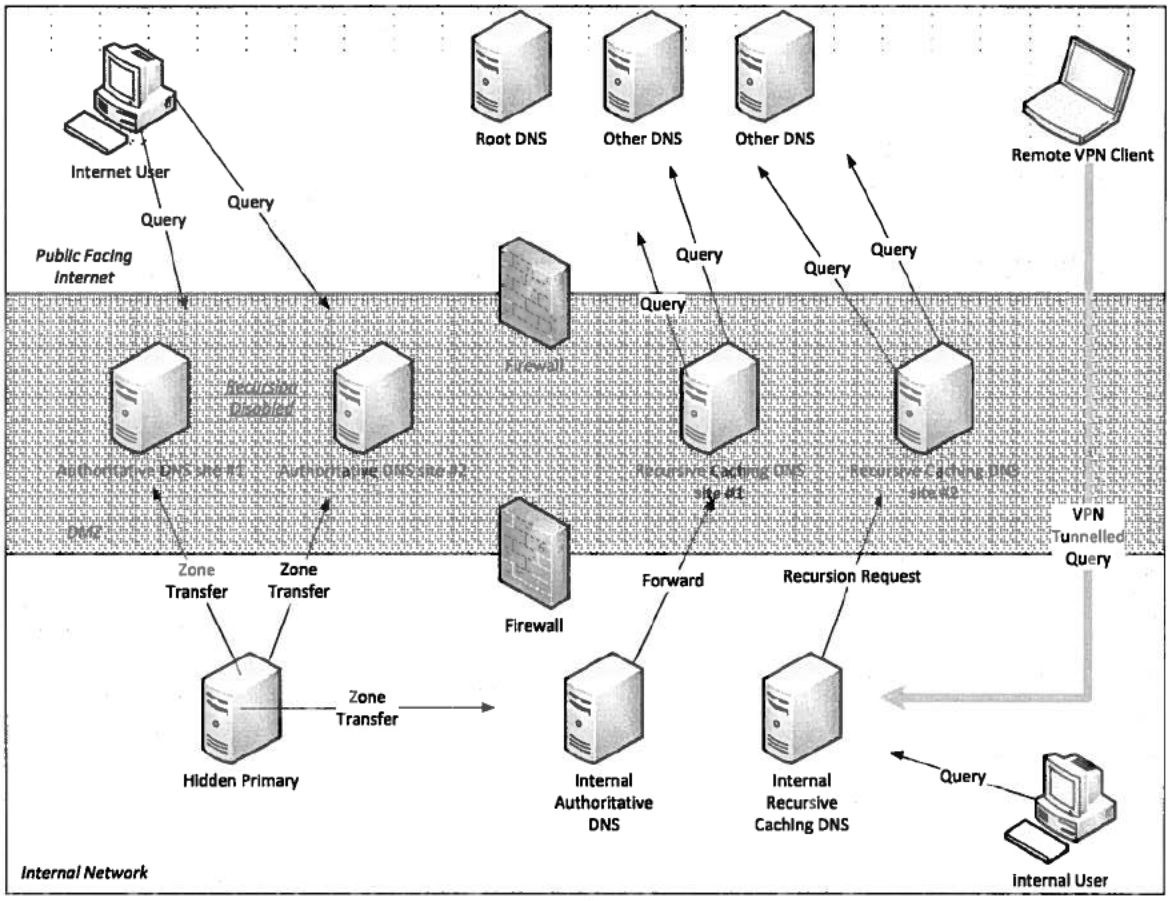
2.3.2 Private Name Server

A name server is private if it does not respond to DNS queries from an external network. Private name servers are positioned inside firewalls as close to internal users as is practical. Private name servers may be authoritative for internal zones or purely recursive caching servers that obtain DNS records from public facing servers.

3 Security Patterns

When planning the DNS infrastructure for an agency, DNS architects should take the respective roles of each name server type into consideration and separate the systems performing each task. Each role has specific usage and security concerns that should be addressed when designing the DNS for the agency. The agency will set up one set of systems for the authoritative service (the left side of Figure 1) and another to provide recursive service for clients within the agency (the right side of Figure 1).

Figure 1: DNS Infrastructure Model



3.1 Authoritative Server Requirements

The basic requirements for an agency's authoritative DNS service are data integrity and high availability in the face of any potential network disruption (intentional or unintentional). A Denial of Service (DoS) attack or network segment break could take the entire agency off line if all of the agency's authoritative servers are located on the same LAN segment. These requirements are met by separating the internal and external authoritative servers (based on the clients they will respond to and the zone information they contain) and dispersing both groups of authoritative servers across different network segments and geographic locations (if possible).

The authoritative servers for the agency should be broken down into two sets: One set to host internal zone data (internal mail servers, application servers, etc.) that resides on the internal network and only responds to other internal hosts, and another set to host externally facing servers that are located on the agency's "demilitarized zone" (DMZ) or Service Network and responds to queries from the external Internet.

Both sets of servers should have all other unnecessary network services uninstalled. Additionally, the authoritative servers located in the DMZ should sit behind the agency's external facing firewall for further protection and only permit allowed necessary ports/protocols.

To ensure the integrity of zone data, DNS administrators should deploy the DNS Security Extensions (DNSSEC) with their zone data. DNSSEC provides source authentication and integrity protection for DNS data through the use of digital signatures. To ensure the integrity of the process, the generation of these digital signatures should be done as close to the authentic data source as possible, with the signed zone then transferred to the hidden primary (for external zones) and internal authoritative zones. More information on how to plan and deploy DNSSEC can be found in NIST SP 800-81r1.

Network administrators should consider using a hidden primary name server for the external DNS authoritative servers. Hidden primary servers make the maintenance of DNSSEC trust relationships much easier in large and complex implementations. A hidden primary is a DNS server that does not appear in the zone data itself as one of the name server records for the zone and yet is the primary server for the zone. The hidden primary is often located behind a firewall and cannot be queried from the external Internet and does not serve zone information to regular users. Its sole function is to host the zone and perform zone transfers to a collection of secondary servers which, in turn are available on the DMZ.

3.2 Recursive Caching Server Requirements

The dedicated recursive servers should also be located within the DMZ. These limited recursive servers should be the only DNS servers allowed to query outside of the agency to retrieve the name resolution.

The dedicated recursive servers should have their access control list tightened to only allow queries from the internal recursive servers. These servers *should not* be accessible from the outside (e.g. through the usage of firewall) as they can be used by attackers as a reflector to launch DDoS attacks. DNS resolution should also be restricted by name as well as IP address.

The dedicated recursive servers should not be used by stub client (resolvers) directly, but through a forwarder. These dedicated recursive servers are also referenced as **forwarders** (or **DNS proxy**), as in other DNS servers forward their queries to these servers to further aggregate the cache. Forwarders also limit the number of DNS servers that are allowed to go out to the Internet to contact external DNS servers. The internal DNS servers (either authoritative or

recursive) that are located in the internal network should accept queries only from the internal hosts.

Usually, these internal recursive DNS servers will be configured to **forward** queries to the dedicated recursive servers located in the DMZ. Normally, the internal DNS servers can be configured to allow full recursion, however, it is recommended that the internal DNS servers only forward and not be allowed to query directly against the root or external DNS servers. For example, when the internal DNS servers cannot resolve entries (e.g. www.website.com), the recursion request is forwarded to the dedicated recursive servers located in the DMZ. The recursive servers will perform the recursion and return the results back to the internal DNS server.

It is recommended that DNS query logging be implemented on the recursive name servers closest to the resolving client. This can be done directly in some DNS implementations as well as by a dedicated network Security Information and Event Manager (SIEM).

For small agencies, one or two recursive servers may be enough. Larger agencies may need several recursive servers and may want to consider having a larger agency-wide aggregate cache (i.e. forwarder) to provide faster response time for users and provide a single gateway for any monitoring by intrusion detection systems (IDS) or similar systems. Separate departments within an agency would have their own recursive server that would forward its queries to the aggregate cache, which would then build an agency-wide cache of responses.

Agencies that perform DNSSEC validation of responses have additional configuration options to consider when setting up recursive systems. At this time, most stub clients (i.e., desktop and laptop systems) do not perform DNSSEC validation, and must rely on a validating recursive server. Therefore, it is important to perform validation as close to the end system as possible to minimize any potential hijack of the response. This risk can be further minimized by the use of IPSec or similar security measures (e.g., DNS transaction signatures; TSIG) for communication between end systems and the validating recursive server.

Administrators also need to configure DNSSEC public keys as trust anchors for one or more zones to enable validation. These trust anchors should be chosen based on a designated security policy. The public key for the root zone should be chosen as one trust anchor, as well as any other zones that the agency wishes to maintain independently.

There are automated protocols and tools to keep trust anchors up-to-date, but initial configuration requires human action. The administrator needs to first identify and obtain the desired trust anchors to install on the validating recursive servers and then establish and monitor a process to perform regular key maintenance. Even though the end nodes may not request DNSSEC validation, DNSSEC validation-enabled recursive servers will perform the chain-of-trust checks starting with available loaded trust anchors. If there is a misconfiguration (e.g. mismatching keys), then the validation will fail, and then subsequent name resolution will fail as well. DNSSEC validation should be enabled with proper operational protocols in place when and if an external site has misconfigured DNSSEC which causes validation to fail for queries to those sites.

4 Systemic Threats & Mitigations

General DNS threats can be categorized into two categories and several sub-categories as discussed in NIST Special Publication 800-81r1: *Secure Domain Name System (DNS) Deployment Guide*. Threats to the **DNS Hosting Environment** include threats to the host platform, the DNS software and the DNS data contents. Threats to **DNS transactions** include threats to DNS queries and responses, threats to zone transfers, threats to dynamic updates and DNSNOTIFY threats. Several checklists are set forth in the NIST publication listing specific mitigation techniques.

Close attention should be paid to the operational context in which DNS servers operate. Not only must they be protected by firewalls and other inherited controls, but DNS server logs should be actively monitored by an integrated security information and event management infrastructure and considered critical information assets by incident response staff.

Table 1: DNS Threats

Threat	Description	Impact
Denial of Service (DoS)	DoS can be initiated intentionally either malicious attacker or unintentionally by a valid user/system. The effect is that the DNS services are overloaded with requests and not able to handle valid requests. DoS can also result when DNS data is incorrectly modified (either maliciously or unintentionally) thus not allowing connectivity to those services.	DoS can make the DNS service unavailable for both authoritative or recursive servers, compromising the availability of the DNS servers.
Cache Poisoning	DNS client is redirected to different set of IP addresses for valid names. The user is not aware that the traffic isn't being directed to the "correct" servers.	Sensitive information such as password can be captured by the attackers, compromising the confidentiality of scores of users.
Compromised Zone transfer data	Zone transfers the full zone from the primary to the secondary. If the transfer isn't secure, the transfer data will be compromised.	The full set of data may be available to malicious attackers, compromising the integrity of the zone information.
Unauthorized Updates	For DNS servers supporting Dynamic DNS Updates (DDNS), the client can issue DDNS update to automatically update the particular zone with data.	Malicious attacker can leverage DDNS to make unauthorized updates against the zone, thus compromising the integrity of the DNS response.

5 DNS Security Configuration

Based upon the concepts developed in previous sections, the following is a brief description of the security capabilities that should be utilized for DNS. These are not new requirements but highlights of existing NIST guidance and standards set forth in NIST Special Publications 800-53, 800-53A, 800-41, 800-81r1 and subsequent publications, federal laws, standards, and guidelines. Industry best practice guidelines are also considered.

5.1 External Authoritative Servers

Table 2: Configuration Summary of External Authoritative Servers

Recommendation	Description	Key Benefits
Use dedicated external name servers	Disable recursion since the name servers should not be performing any recursion.	Eliminate cache poisoning.
Disperse name servers	Name servers should be spread across multiple switches and sites to minimize the impact of outages. Larger sites may Use wide-area routing protocol strategies, such as Anycast, to balance query loads across many geographically disbursed servers.	Increase availability Site resiliency.
Utilize DNS resolution blocking and logging	BIND 9.3 is an example with capabilities such as allow query list, recursion allowed list, etc.	Tighten security control.
Turn off all services except for DNS	Remove any unnecessary software / services running from the external DNS authoritative servers.	Minimize DoS. Minimize impact of security vulnerabilities of other services.
Restrict access to DNS ports to outside users	Use a Firewall system to further prevent access to the servers.	Minimize DoS. Increase defense depth.
Use hidden primary	Place the primary server that is hidden (no NS record) inside the firewall. All changes on the zones are made on the primary and transferred.	Minimize configuration errors leading to DoS. Eliminate DoS targeting primary servers for zones.
Use authenticated zone transfers	For each secondary server, use a unique Transaction SIGnature (**TSIG**) key or some other means to authenticate zone transfers (e.g. IPSec).	Compromised Zone transfer data.
Disable DDNS	External DNS servers do not allow DDNS.	Eliminate Unauthorized DNS updates.
Enable DNSSEC to	DNSSEC provides integrity of the records	Minimize cache

sign zones	by signing each record set with the private key and publishing the public key via DNSSEC record. DNSSEC validating servers can then use the public key stored in the DNSSEC record to decrypt the signature to validate the integrity of the DNSSEC record(s).	poisoning.

5.2 Recursive Caching Servers

Table 3: Configuration Summary of Recursive Caching Servers

Recommendation	Description	Key Benefits
Use dedicated recursive servers	No authoritative zones will be "hosted" on the recursive servers.	Isolate name server functions.
Disperse name servers	Name servers should be spread across multiple switches and sites to minimize the impact of outages.	Increase availability. Site resiliency.
Place recursive servers at the DMZ	These become "DNS" Proxy servers as many organizations do not allow DNS traffic to go directly from the internal network to the "outside". By leveraging forwarding, the DNS proxy (recursive) servers will fetch the name resolution and return it back to the original resolver.	Maintain tighter security boundary.
Restrict access to internal users	The DNS traffic will always originate from recursive servers, and never from outside TO the recursive servers. We lock down these servers from being 'reachable' from outside world.	Minimize DoS Eliminate our servers being hijacked by attackers to perform DoS against others.
Restrict access to legitimate domains	Recursive DNS servers can be configured to disallow and/or log attempts to resolve certain domains. This can be done either in place of or as part of an integrated Data Loss Prevention (DLP) solution.	Increase site security/Minimize threats to internal hosts.
Define recursion-list	Although recursion is enabled, the recursion-allowed list should be tightly set so that only a small set of systems can send queries to the recursive server.	Minimize DoS. Eliminate our servers being hijacked by attackers to perform DoS against others.
Define query-list	This is similar to the recursion allowed list. Only a small set of IP's should be allowed to query these servers.	Tighter control. Minimize DoS vectors.
Enable DNSSEC Validation	Once DNSSEC is deployed more widely, DNSSEC validation takes advantage of	Eliminate cache poisoning.

	the signed zones by validating not only the chain of trust (root servers and down) but also the validity of each record.	

5.3 Internal Authoritative DNS servers

Table 4: Configuration Summary of Internal Authoritative Servers

Recommendation	Description	Key Benefits
Set up DNS forwarding	The internal authoritative servers should only forward DNS queries to the dedicated recursive servers. These should not be allowed to recurse or query outside.	Isolate name server functions. Maintain tighter security boundary.
Disperse name servers	Name servers should be spread across multiple switches and sites to minimize the impact of outages.	Increase availability. Site resiliency.
Define query-list	This is similar to the recursion allowed list. Only the internal clients should be listed on the query list.	Tighter control. Minimize DoS.
Block Access from Outside	The internal name servers should not be reachable from the outside world.	Minimize DoS.
Use "hidden" primary name server	Although hidden primary isn't as important as it is for external name servers, it still adds value by minimize the impact of misconfigured primary servers on the secondary servers.	Minimize configuration errors leading to DoS.
Evaluate DNSSEC	Most organizations are not yet ready for DNSSEC for internal zones. The agency should at least evaluate what needs to be done, what hurdles need to be overcome to implement DNSSEC. By evaluating its readiness, the agency can make the necessary steps to move toward them.	Eliminate cache poisoning. Maintain DNS integrity.

6 Implementation Considerations

The following sections provide implementation considerations for VPN clients, security policy, outsourcing, and DNSSEC signing and validation. In addition to the considerations listed here for DNSSEC signing and validation, the Federal CIO Council publication on *Considerations for Federal Agency Implementation of DNS Security Extensions and Email Authentication* may provide further information to agencies when implementing DNSSEC.

6.1 Remote VPN Clients

Administrators need to provide one or more recursive servers for remote users connecting back to the agency's network via a VPN. Mobile users may not be able to trust the recursive server provided by the remote network. Also, the remote network's recursive server(s) may not perform DNSSEC validation and if validation is performed, mobile users will not know what trust anchors are used. Mobile users should have a means to connect back to the home agency's network and use one of the trusted recursive servers (or a special recursive server for VPN users).

6.2 DNS and Security Policy

Under FISMA, critical information technology resources are configured and evaluated as parts of General Support Systems (GSS's) and applications, both major and minor with differing respective configuration and auditing guidance. Because DNS affects every existing GSS, often in multifaceted ways, changes to DNS will have repercussions to those existing systems. It is therefore recommended that agencies consider establishing DNS as a separate GSS under FISMA rules. This makes it much easier to evaluate the effect of major changes (such as implementing DNSSEC) on other critical infrastructure elements prior to ratifying changes.

Because DNS is involved in virtually every network transaction, DNS servers should be characterized as both highly critical and highly sensitive under FISMA guidance.

6.3 DNS Outsourcing

Agencies may choose to outsource all or part of their DNS infrastructure. The reasons for doing so are that trusted third parties may be better able to provide the security, geographical dispersion and high-availability safeguards than an internal network data center. There also may be cost considerations.

Outsourcing DNS infrastructure, however, does present drawbacks. Not only can it complicate remote administration, but it may subject the agency to security attacks leveled at the outsourced organization. It may also make it difficult to monitor recursive servers close to internal users. The nature of DNS also makes a hybrid solution possible where part of the DNS is hosted internally and the external facing DNS is hosted either all or in part by a trusted third party.

It is therefore recommended that agencies consider both the costs and benefit of an outsourced approach when designing their DNS architecture.

6.4 DNSSEC Signing

Secure DNS architecture is complex and difficult to implement. Network administrators should consider multiple facets of DNSSEC when planning an implementation. The following is a set of implementation recommendations with corresponding issues for administrators to consider for a successful implementation of DNSSEC.

The DNSSEC signing is mandated through OMB Mandate M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*. The DNSSEC signing is only mandated for the external DNS zones and not for internal DNS zones. A first task for the administrator is to evaluate the current external name server.

The following are some questions that should be answered about the existing implementation prior to implementing DNSSEC signing.

Table 5: Implementing DNSSEC Signing

Questions	Steps to Resolve
Can our current external name servers support DNSSEC?	Check the current versions and confirm that the DNSSEC signing is supported. The primary server must supporting DNSSEC signing while the secondary/slave only needs to support DNSSEC records. Review different options to deploy DNSSEC. If your current DNS environment cannot support DNSSEC, review the options (e.g. upgrade, replace, or outsource).
Will our Firewall configuration support DNSSEC?	DNSSEC records are larger than the typical DNS records. DNSSEC packets can be as big as 4096 bytes and sometimes TCP is used as a transport instead of UDP. For DNS servers sitting behind the FW, the setting for packet must be reviewed and tested. Firewalls should be set to allow DNS traffic to use both TCP and UDP on port 53.
What exactly are our available DNSSEC capabilities?	The encryption level and the NSEC3 capability should be reviewed carefully before signing the zone. Once the zone is signed with particular encryption level and/or NSEC3, changing the setting requires a set process of resigning zone data, which can be difficult. Review the various signing options and select the ones that meet the requirements.
Can we automate DNSSEC	DNSSEC adds layer of administration that requires

administration?	considerable amount of time to do day-to-day functions such as adding or updating a DNS record. Consider automated scripts or automated tools to streamline the signing of the records as well as zone/key singing key roll-over process.
What do we do with the DNSSEC private key?	As with any PKI related products, the private key that signs the records must be maintained in a secure place. Once the key is compromised, all records must be unsigned and resigned with a different key. Develop methods to secure the private key. Identify and minimize who will have the access to the key.
How do we roll-over DNSSEC Keys?	While the KSK (key signing key) rollover is 1 year (recommended), the ZSK (zone signing key) is recommended to roll-over every month. Rolling over ZSK will be a considerable effort if done manually. Automate the zsk roll-over process by either scripting or implementing an automated tool.
How do I test DNSSEC signing?	Before signing your production zones, a pilot zone can and should be signed first to confirm the functionality. Visit http://www.dnsops.gov/ and participate in the pilot program.

6.5 DNSSEC Validation

DNSSEC validation is not covered under the current OMB Mandate M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*. However, it should be considered as part of the DNSSEC implementation.

Table 6: Implementing DNSSEC Validation

Questions	Steps to Resolve
How do we set the Root Trust-Anchor?	Chain-of-anchor must be set manually (and out-of-band). The IANA website (https://www.iana.org/dnssec/) publishes the root zone DNSSEC trust anchor. Document and test the steps to load the trust anchor from the website into your recursive servers.
How do we avoid DNSSEC validation problems?	When other agencies make a DNSSEC configuration errors such as letting signatures expire or mismatching the DS and DNSKEY records, the result will be that your DNSSEC validation enabled servers will not able to resolve anything from the other agencies DNS server. Define a protocol on what will be done if and when misconfiguration or DNS attack is identified.
How will DNSSEC affect Recursive Server	DNSEC validation will require additional processing power on your recursive servers. Obtain performance baseline

performance?	before validation is turned on and compare the performance metrics after the validation is enabled.

APPENDIX A: Acronyms – Common Abbreviations

ACL - Access Control List

BIND - Berkeley Internet Name Domain

CIO - Chief Information Officer

DDNS - Dynamic Domain Name System

DDoS - Distributed Denial of Service

DMZ – De-Militarized Zone

DNS - Domain Name System

DNSSEC - Domain Name System Security Extensions

DoS - Denial of Service

FIPS - Federal Information Processing Standards

FISMA - Federal Information Security Management Act

FW – Firewall

GSA - General Services Administration

IDPS - Intrusion Detection and Prevention Systems

IDS - Intrusion Detection System

IPS – Intrusion Prevention System

IP - Internet Protocol

ITILoB - Information Technology Infrastructure Line of Business

KSK - Key Signing Key

LAN - Local Area Network

NIST - National Institute of Standards and Technology

NSEC3 - Next Secure

NSTIC – National Strategy for Trusted Identities in Cyberspace

OMB - Office of Management and Budget

PKI - Public Key Infrastructure

RR – Resource Record

TCP - Transmission Control Protocol

TIC - Trusted Internet Connections

TSIG - Transaction Signature

UDP - User Datagram Protocol

VPN - Virtual Private Network

WG - Working Group

ZSK - Zone Signing Key

APPENDIX B: Glossary – Common Terms and Definitions

Authoritative Server: A server that knows the content of a DNS zone from local knowledge, and thus can answer queries about that zone without needing to query other servers.

Berkeley Internet Name Domain (BIND): BIND is the most commonly used implementation of the Domain Name System (DNS) protocols. BIND provides a robust and stable platform on top of which organizations can build distributed computing systems with the knowledge that those systems are fully compliant with published DNS standards.

Cache: A component that transparently stores data so that future requests for that data can be served without contacting the original host.

Cache Poisoning: A malicious attack that compromises the integrity of DNS by redirecting the domain to a different IP address.

Demilitarized Zone (DMZ): The DMZ (or Service Network) is a perimeter network segment that enforces the internal network information assurance policy for external information exchange.

Denial of Service (DoS): Intentionally or unintentionally overloading a computer resource to make a service unavailable.

DNS Security Capabilities: Requirements that cover industry best practice security measures for DNS

Domain Name System (DNS): DNS is a hierarchical, distributed database for any resource connected to the Internet or private network that translates readable domain names to IP addresses.

Domain Name System Security Extensions (DNSSEC): DNSSEC is a suite of specifications that provides origin authentication, authenticated denial of existence, and data integrity to DNS clients (resolvers). DNSSEC was designed to prevent cache poisoning and does not provide services for availability or confidentiality.

Intrusion Detection: The process of monitoring the events occurring in a computer system or network and analyzing them for signs of potential incidents.

Intrusion Detection and Prevention System (IDS/IPS or IDPS): Identifies potential incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Intrusion Prevention: The process of performing intrusion detection and attempting to stop detected potential incidents.

Listed Server: An Authoritative Server for which there is an NS resource record (RR) in the zone.

Name Server (NS): Provides responses to name resolution queries. An authoritative name server for a zone provides responses to name resolution queries for resources for that zone, using the Resource Records (RRs) in its own zone file.

NSEC3: The purpose of an NSEC (Next Secure) record is to prove that no records exist between two different points. NSEC3 records use hashes to prevent queries from reporting what records do exist.

NSTIC: The National Strategy for Trusted Identities in Cyberspace is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions.

Primary Server: An authoritative server for which the zone information is locally configured. A Primary Server is also known as a Master Server.

Public Facing Name: A name server which responds to queries from external networks.

Private Name Server: A name server which does not respond to queries from external networks.

Recursive Caching Name Server: A server that combines both caching and recursive functions in the same Name Server. These servers store DNS query results for a period of time (caching), and also implement the recursive algorithm necessary to resolve a given name starting with the DNS root through to the authoritative name servers of the queried domain. The combination of these two functions in one name server is not mandatory; the functions can be implemented independently in servers for special purposes

Recursion: A method of defining functions (or protocols) in which the function being defined is applied within its own definition.

Resolver: A client of the DNS which seeks information contained in a zone using the DNS protocols.

Resource Records (RRs): RRs are the basic data elements in the domain name system. RRs translate Domain Names to IP addresses. When sent over an IP network, RRs use the common format specified in RFC 1035 (NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA).

Secondary Server: An authoritative server that obtains information about a zone from a Primary Server via a zone transfer mechanism. A Secondary Server is also known as a Slave Server.

Server: An implementation of the DNS protocols able to provide answers to queries. Answers may be from information known by the server, or information obtained from another server.

Stealth Server: An authoritative server, usually a secondary server, which is not a Listed Server.

Transaction Signatures: Transaction signatures provide a means of authenticating queries between servers, including updates to a Dynamic DNS database. TSIG uses shared secret keys and one-way hashing to provide a cryptographically secure means of identifying each endpoint of a connection as being allowed to make or respond to a DNS update.

Transmission Control Protocol (TCP): TCP provides reliable, ordered delivery of a stream of bytes on an Internet Protocol (IP) network from a program on one computer to another program on another computer. TCP, along with UDP, are the two core Network Protocols in the Internet Protocol Suite.

User Datagram Protocol (UDP): UDP allows computer applications to send messages (datagrams) to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. UDP, along with TCP, are the two core Network Protocols in the Internet Protocol Suite.

Zone: A DNS zone is a portion of the global DNS namespace for which administrative responsibility has been delegated.

Zone Transfer: A DNS function used to replicate DNS databases across other DNS servers.

APPENDIX C: Selected Existing Guidance

The origin for this initiative is OMB M-08-23. The following OMB Memoranda impact this Reference Architecture:

- OMB M-08-23: *Securing the Federal Government's Domain Name System Infrastructure*

A comprehensive list of applicable legislation, policies, directives, regulations, memoranda, standards, and guidelines can be found in the following:

LEGISLATION

E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

National Security Presidential Directive (NSPD) 54, *Cyber Security and Monitoring*, 8 January 2008. Also known as HSPD-23.

Homeland Security Presidential Directive (HSPD) 23, *Computer Network Monitoring and Cyber-security*, 8 January, 2008. Also known as NSPD-54.

Office of Management and Budget (OMB) Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, 2 August 2005.

Office of Management and Budget (OMB) Memorandum *M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, 11 January 2007.

Office of Management and Budget (OMB) Memorandum M-08-05, *The Trusted Internet Connection initiative (TIC)*, November 2007.

National Security Telecommunications And Information Systems Security Committee NTTISSP 101, *National Policy on Securing Voice Communications,* 14 September 1999.

STANDARDS

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

General Services Administration (GSA), Public Buildings Service (PBS), *Facilities Standards (P100)*, 2009.

Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Module*, 3 December 2002.

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

Federal Information Processing Standard (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2006.

IEEE 802.1X: IEEE Standard for port-based Network Access Control (PNAC).

GUIDANCE

Federal CIO Council, *Considerations for Federal Agency Implementation of DNS Security Extensions and Email Authentication,* June 2011.

NIST's Information Technology Laboratory, ITL Security Bulletins, *An Introduction to Secure Telephone Terminals - ITL Security Bulletin*, March 1992.

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010.

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

National Institute of Standards and Technology Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*, December 2010.

National Institute of Standards and Technology Special Publication 800-81, Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, April 2010.

National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

Office of Management and Budget Memoranda, M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, 4 April 2008.

Office of Management and Budget Memoranda, M-08-26, *Transition from FTS 2001 to NETWORX*, 28 August, 2008.

Office of Management and Budget Memoranda, M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*, 20 September 2008.

Office of Management and Budget Memoranda, M-09-32 *Update on the Trusted Internet Connections Initiative*, 17 September 2009.

Federal Network Security
Federal Interagency Technical Reference Architectures

Electronic Mail Gateway Security Reference Architecture

Version 1.0

12/12/2011

Department of Homeland Security
National Cyber Security Division
Federal Network Security
Network & Infrastructure Security

Revision History

Date	Version	Description	Approved By
12/12/2011	1.0	Initial Version	CS&C

Table of Contents

ACKNOWLEDGEMENTS 1

STAKEHOLDERS 1
PARTICIPANTS 1

1 PURPOSE AND SCOPE 2

2 ELECTRONIC MAIL GATEWAY ARCHITECTURAL COMPONENTS 2

2.1 SYSTEM OVERVIEW 3
2.2 INBOUND MAIL TRANSFER AGENT (MTA) 4
2.3 OUTBOUND MAIL TRANSFER AGENT (MTA) 4
2.4 BILATERAL MAIL RELAY/EXCHANGER (MTA) 5
2.5 MOBILE MESSAGING 5

3 SECURITY PATTERNS 5

3.1 SECURITY USE CASES 5
3.1.1 Pattern 1: Inbound Electronic Mail 5
3.1.2 Pattern 2: Outbound Electronic Mail 6
3.1.3 Pattern 3: Mobile Messaging 6
3.2 SECURITY ARCHITECTURE COMPONENTS 6
3.2.1 Pipeline Structure 7
3.2.2 Data Loss Prevention 11
3.2.3 Content Compliance 11
3.2.4 Malware Filtering 11
3.2.5 Domain Validation 12
3.2.6 SPAM Filtering 12
3.2.7 Agency Specific Modules 12
3.3 SECURITY REQUIREMENTS 13
3.3.1 Inbound Gateway Mail Transfer Agent (MTA) Requirements 13
3.3.2 Outbound Gateway Mail Transfer Agent (MTA) Requirements 13
3.3.3 Mail Submission Agent Requirements 14
3.3.4 Mail Delivery Agent Requirements 14
3.3.5 Mail User Agent Requirements 14
3.3.6 Domain Name System (DNS) Requirements 14
3.3.7 Firewall Requirements 15
3.3.8 Logging Requirements 15
3.3.9 System Monitoring and Control 16
3.3.10 Archiving Requirements 16
3.3.11 Audit Requirements 16

4 SYSTEMIC THREATS & MITIGATIONS 16

5 SECURITY CONFIGURATION 22

6 APPENDIX A: SAMPLE SPF RECORDS 23

7 APPENDIX B: SAMPLE DKIM DOMAIN RECORD ENTRY 24

8 APPENDIX C: ACRONYMS – COMMON ABBREVIATIONS 26

9 APPENDIX D: GLOSSARY – COMMON TERMS AND DEFINITIONS 28

10 APPENDIX E: SELECTED EXISTING GUIDANCE 32

10.1 LEGISLATION 32
10.2 POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA 32

10.3 STANDARDS 32
10.4 GUIDELINES 33
10.5 IETF RFCs 36

Figures

FIGURE 1 - MAIL SYSTEM FUNCTIONAL COMPONENTS 4
FIGURE 2 - SMTP TRANSFER MODEL 7
FIGURE 3 - INBOUND MTA PIPELINE 8
FIGURE 4 - OUTBOUND MTA PIPELINE 10

Acknowledgements

This document is the product of a multi-agency collaboration to provide guidance for the successful and secure implementation of Electronic Mail Gateways at Federal civilian agencies. It further expands on the Critical and Recommended Content Filtering capabilities found in the Trusted Internet Connections (TIC) Reference Architecture v2.

This document will be reviewed annually and updated when necessary to incorporate required capabilities and applicable interoperability standards.

Stakeholders

All Federal civilian agencies
Office of Management and Budget (OMB), Office of E-Government and Information Technology
Federal Chief Information Office (CIO) Council
Federal Small Agency CIO Council
Department of Homeland Security (DHS) National Cyber Security Division (NCSD)
Federal Systems Security Governance Board (FSSGB)
DHS Information Systems Security Line of Business (ISS LoB)
DHS United States Computer Emergency Readiness Team (US-CERT)
General Services Administration (GSA) Information Technology Infrastructure Line of Business (ITI LoB)

Participants

Name	Agency	Name	Agency
Jim Quinn	DHS	Eric Pratsch	SRA-Touchstone
Marilyn Rose	DHS	Robert Moore	SRA-Touchstone
Oscar Ahumada	DHS	Marcos Evangelista	STATE
Sean Donelan	DHS	Janice Ousley	Treasury/IRS
Arthi Appulingam	EDU	Stewart Grossman	Treasury/IRS
David Elliot	EDU	Homa Zarrinnahad	Treasury/OCC
Pete Batista	FCC	Tim Arnold	USDA
Daniel Sheehan	Indian Health Service		
Jeff Schwefler	MITRE		
Carl Beaudry	SRA International		

1 Purpose and Scope

On April 15, 2011, the White House released the National Strategy for Trusted Identities in Cyberspace (NSTIC), which envisions the establishment of secure online identity functionality as part of an overall cyber security strategy. The purpose of the Mail Gateway Reference Architecture is to improve and standardize the Electronic Mail Gateways currently in use by the Federal Civilian Government, help Departments/Agencies (D/As) comply with FISMA mail security requirements and to improve the Federal Government's overall security posture by reducing electronic mail vulnerabilities.

This document is a reference that provides insight and guidance for D/As implementing an electronic mail gateway. This document is descriptive in nature, recognizing that many organizations face unique challenges that do not lend themselves to a "one size fits all" solution. Unlike a Target Architecture, a Reference Architecture does not mandate specific solutions, but rather identifies a range of workable modular solutions. The intent is to enable agencies to leverage existing best practice solutions when implementing electronic mail gateways. The reference architecture will align with the National Strategy for Trusted Identities in Cyberspace (NSTIC), the evolving Anti-Phishing policy, and the National Cyber Security Strategy while factoring in the context of each organizations respective missions, programs, and initiatives.

This document is intended for use by Federal civilian agencies. The information in this document is based upon collaboration with multiple agencies, the definitions and requirements in the Federal Information Systems Management Act (FISMA), National Institute of Standards and Technology (NIST) guidance and standards, Trusted Internet Connection (TIC) Reference Architecture v2, Office of Management and Budget (OMB) memoranda, and evolving national cyber security policies.

2 Electronic Mail Gateway Architectural Components

An Electronic Mail Gateway provides the interface between federal agencies' internal mail systems and the mail systems of other federal agencies or Internet mail systems. The gateway processes inbound and outbound mail messages. The complete mail ecosystem which encompasses the mail gateway as well as other components is represented by:

- Mail User Agents (MUAs)/e-mail clients
- Mailbox hosts
- Mail Submission Agents (MSAs)
- Mail Delivery Agents (MDAs)
- Mail Transfer Agents (MTA) both inbound and outbound
- Mail Exchangers
- Mobile messaging servers

- Applications Servers

The electronic mail gateway reference architecture focuses on the MTAs (Figure 1 filled in black) but for architectural completeness the boundaries to the other components are included here.

2.1 System Overview

The electronic mail system provides both inbound and outbound mail transactions.

For the outbound transaction, the electronic mail client/MUA provides the user interface, the MSA stores and forwards electronic mail messages to the MTA which, in turn, acts as a proxy between the MSAs and external mail servers.

For the inbound transactions, the MTA receives the messages, the MDA stores the messages, and MUA/mail client provides user access to the message stores. The mobile messaging server provides a secure connection between the mobile messaging device and the MDA and MSA.

Security controls placed on the inbound and outbound MTA pipelines are applied to both mobile and traditional mail transactions. Agency-hosted applications requiring the ability to send email are considered application servers which may deliver outbound mail to either the MSA or the outbound MTA. Application servers may also receive inbound email from either the MDA or inbound MTA. For completeness, mailbox hosting is depicted as a capability connected to the MSA and MDA.

The Electronic Mail Gateway is divided into inbound and outbound MTA pipelines. The relationship of the components and the alignment with the TIC Reference Architecture v2 is depicted in *Figure 1* below. The focus of the Electronic Mail Gateway reference architecture is to describe the functions of inbound and outbound MTAs with reference to the other components of the mail handling system. In addition, the Mail Gateway Reference Architecture relies on functionality described in the Domain Name System (DNS) Security Reference Architecture to discover both internal and external mail handling hosts and the functionality described in the TIC Reference Architecture v2 to provide DMZ functionality.

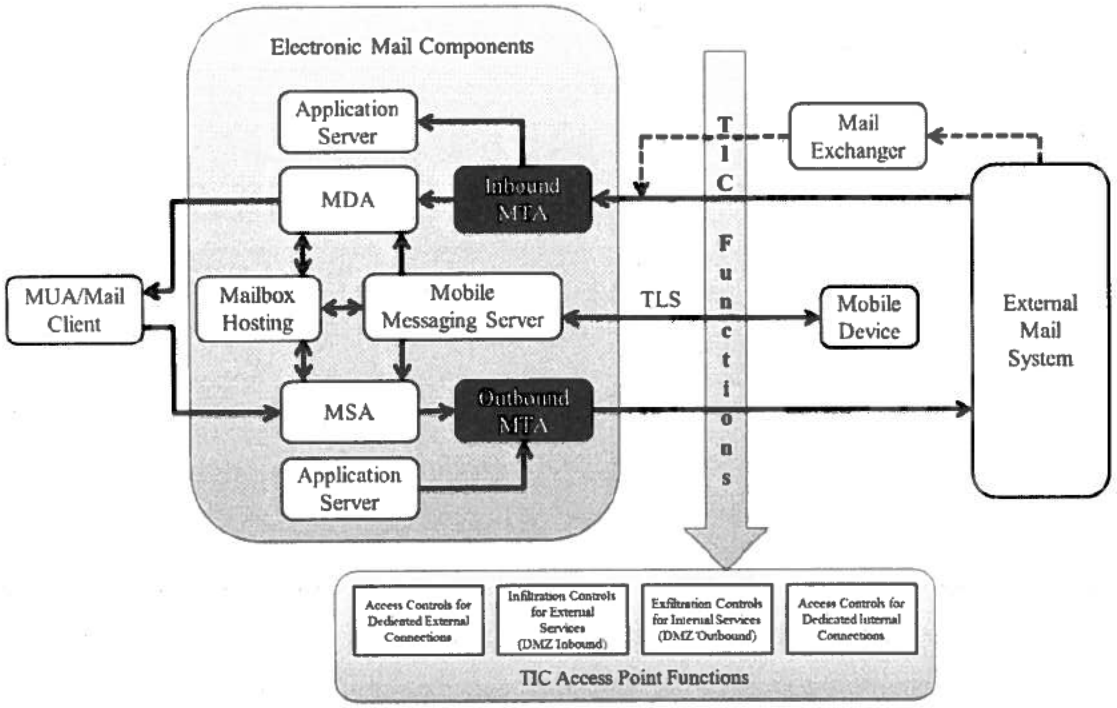


Figure 1 - Mail System Functional Components

2.2 Inbound Mail Transfer Agent (MTA)

The inbound MTA processes all mail originating from outside the federal agencies' network. For the Electronic Mail Gateway reference architecture, the enclave represents all users operating within the federal agencies network to include users that are connected by a Virtual Private Network (VPN) or other form of remote connection. The inbound MTA performs functions such as domain validation, spam filtering, malware filtering, and any other agency unique modules. Based on the findings of each function, the MTA will make a disposition decision for each inbound mail transaction. Depending on the sender's security capabilities and receiver's security requirements, the inbound MTA will enable server to server mandatory and/or opportunistic encryption services.

2.3 Outbound Mail Transfer Agent (MTA)

The outbound MTA processes all mail originating from inside the federal agencies' enclave. The purpose of the outbound MTA is to provide domain validation, content compliance, data loss prevention, malware filtering, and any other agency unique modules. By providing appropriate outbound controls, the systems acts as a good steward of federal and Internet network resources by reducing the risk to external electronic mail systems as well as providing a

monitoring interface for Data Loss Prevention (DLP) services, encompassing both spam and malware filtering of mail transfers. The outbound MTA functions are self-adjusting depending on the target external mail system and agency policy. For example, electronic mail between federal agencies may be handled differently than mail destined for Internet mail systems. Based on the findings of each function, the MTA will make a disposition decision for each outbound mail transaction. Depending on the agency security policy, the outbound MTA will opportunistically enable server-to-server encryption services wherever possible.

2.4 Bilateral Mail Relay/Exchanger (MTA)

The bilateral mail exchanger provides an optional proxy capability which enables the pre-collection of electronic mail. Large sites may choose to employ a mail exchanger outside of their enclave which, in turn, routes mail to multiple inbound and outbound electronic mail gateways. This configuration provides a mechanism to outsource the mail exchange function as well as some mail pipeline functions. By implementing external mail exchangers, disaster recovery and business continuity functions are also supported by storing incoming and outgoing mail in a trusted location during enclave mail system outages.

2.5 Mobile Messaging

Many agencies require connection to a mobile device mail system. For example, an agency may require Blackberry electronic mail services provided by a Blackberry Enterprise Server (BES) or Android/iOS services provided by the Microsoft ActiveSync protocol. (The reference architecture does not advocate any particular mobile messaging service but recognizes the prominent position of these protocols in the federal workplace.) Mobile messaging servers communicate via an external network to mobile devices and, in turn, the mobile messaging server sends and receives electronic mail via the inbound and outbound MTAs. The mail gateway reference architecture does not describe the mobile messaging architecture in detail except for the interface of the mobile architecture with the mail gateway pipeline.

3 Security Patterns

The operation of the electronic mail gateway is described by first identifying common use cases then identifying the functions of the security architecture required to meet federal security requirements.

3.1 Security Use Cases

3.1.1 Pattern 1: Inbound Electronic Mail

The Inbound Electronic Mail security pattern consists of all inbound mail originating outside the agencies' enclave. The security pattern does not differentiate between electronic mail arriving from trusted or unknown sources. All mail will pass through an inbound pipeline and be processed by agency policy. The theory is that the inbound pipeline components are the same regardless of source.

3.1.2 Pattern 2: Outbound Electronic Mail

The Outbound Electronic Mail security pattern consists of all outbound electronic mail originating from within the sending agencies' enclave. This includes mail being sent to trusted, untrusted, or unknown trust level destinations. The operational concept is all outbound mail will pass through the same outbound pipeline. The pipeline might be tuned for specific destinations but the pipeline components will not change.

3.1.3 Pattern 3: Mobile Messaging

The Mobile Messaging security pattern describes the condition where the electronic mail gateway needs to send or receive mail from a commercial mobile messaging system. The mobile messages must fully participate in the electronic mail gateway. The mobile messaging reference architecture will be described in a separate reference architecture but it is included here to describe the interaction with the electronic mail gateway reference architecture.

3.2 Security Architecture Components

The normal flow of Simple Mail Transport Protocol (SMTP) mail is illustrated in Figure 2 below. Electronic mail gateways consist of both mail transfer agent (MTA) and Mail Exchanger (MX) functions implemented over one or more agency mail servers. Ideally mail server functions are divided over multiple redundant hosts to better assure high availability and security encapsulation.

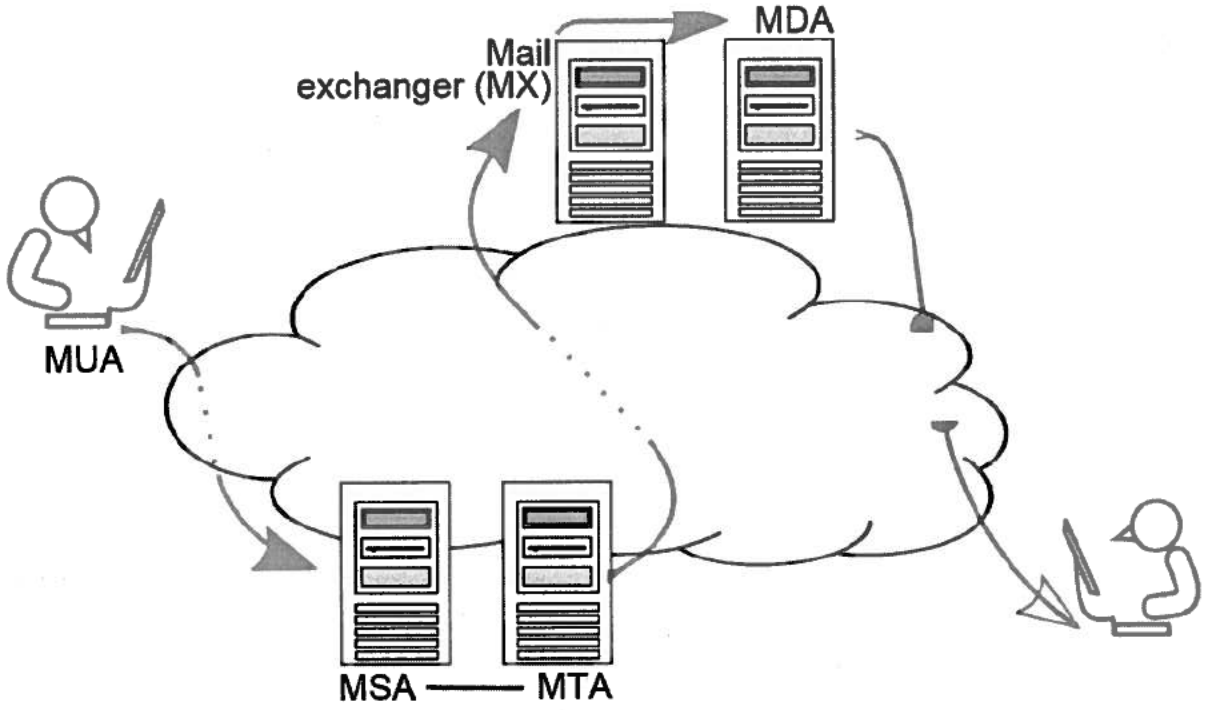


Figure 2 - SMTP Transfer model

Because the functions of mail gateways are heterogeneous at the source and destination sites, they should be configured differently depending on whether they are to hand inbound or outbound electronic mail. It should also be noted that multiple hosts may be configured to perform each function depending on capacity requirements.

3.2.1 Pipeline Structure

The email gateway should be configured in a modular fashion which allows for the provision of additional mail security controls as well as redundant hosting of mail services. Incoming and outgoing mail must be routed through a pipeline architecture consisting of one or more servers performing the designated electronic mail handling functions

A series of functions are performed on the message as it passes through an inbound or outbound MTA. The MTA provides anti-spam functions, data loss prevention, content compliance, malware detection, and domain validation. Depending on agency security policies, one or more additional functions can be inserted into the mail processing pipeline. Policy enforcement will also dictate what actions or logging is required for each pipeline component. A representation of an inbound and outbound MTA pipeline is shown in Figure 3 and 4. The advantage of a pipeline is that additional processes can be added and it is not constrained to a single vendor solution.

Depending on agency policies, the MTA pipelines should be linked to the agencies archiving functions and policies.

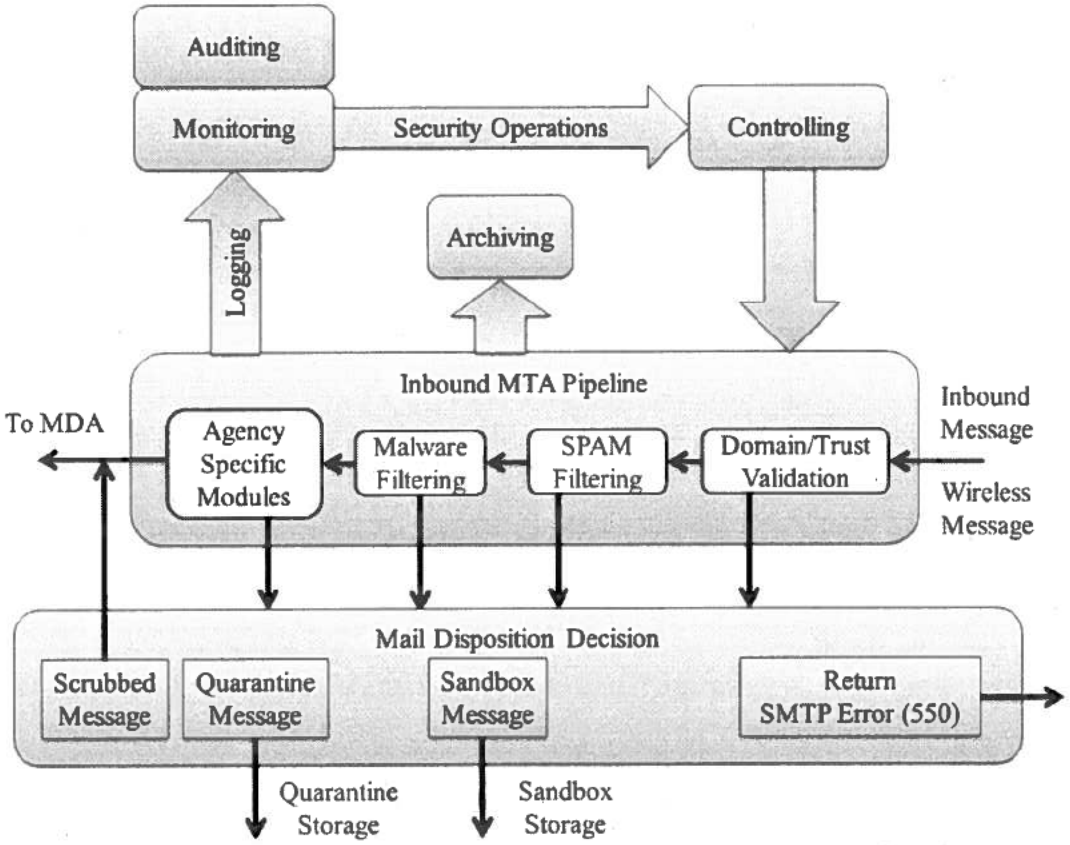


Figure 3 - Inbound MTA Pipeline

Also, in order to provide electronic mail gateway monitoring and control visibility, the MTA pipeline components must provide status information via logging to a monitoring function. The specific agency policies will dictate how the logging information is used but it is especially important to consider logging, monitoring, controlling, archiving, and auditing when outsourcing any function of the MTA pipelines.

The order of pipeline functions is critical to the efficient operation of the pipeline. The design objective is to perform the most effective and least resource intensive functions first. In the case of the inbound pipeline, domain validation provides a quick method to filter incoming messages by the level of trust established by an individual sender. This necessitates making disposition decisions on each mail message as soon as possible.

The current proportion of SPAM received by a conventional inbound mail pipeline makes rejecting suspected SPAM early in the pipeline critical. By filtering SPAM early, fewer messages need to be processed by more resource-intensive malware filters. Many security vendors have developed sophisticated SPAM filters which are based on proprietary data collection techniques and it is important to note, the frequency of SPAM filter updates when choosing a vendor solution.

Because SPAM attackers have the option to run short-duration attacks which "fly under the radar" of update cycles, agency solutions need to use any bad IP address, domains, or filters published by the US CERT to make a mail disposition decision. The decision criteria will be based on agency policies as well as technical capabilities. At a minimum, the inbound pipeline will support scrubbing messages, quarantine, and the issuance of SMTP 550-series error messages. The SMTP 550 reply code is generic: "Requested action not taken: mailbox unavailable". This reply condition provides minimal information to SPAM and malware senders but provides enough information to legitimate sending servers that something is wrong.

Each module in the inbound mail pipeline will either pass the message to the next module or execute a mail disposition event. Final disposition either results in the mail being rejected with a SMTP error code of 550, being moved to a quarantine, being scrubbed and delivered to the user, or being moved to a sandbox. The reject option must return a code of 550 to prevent the sender from being able to derive account information from the MTA. The quarantine and sandbox both prevent delivery of the message to the MUA but the handling of the message is different. In the case of quarantine, the message is stored and an appropriate message is delivered alerting the user on how to view the message without retrieving it. The sandbox opens the message trying to determine risk of any message content. If the message is determined to be safe the message can be returned to the user. The scrubbing option removes any detected problems and delivers the message to the MUA. As an example, the scrubber might remove an attachment that is deemed to be high risk and replace it with an appropriate message. A frequently seen case is the removal of executable attachments.

For the inbound pipeline all of the modules must be included. If a portion of the pipeline is outsourced, all modules must be accounted for using either outsourced or organic resourced. The mail disposition instruction system must support the return function but the agency can implement any combination of the scrubbing, quarantining, or sandboxing of messages but at least one must be used.

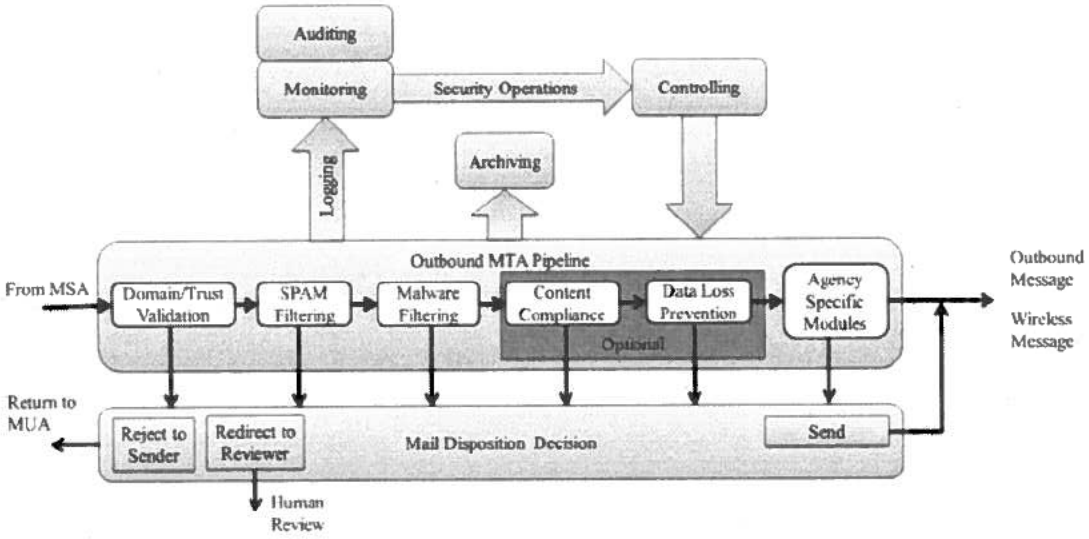


Figure 4 - Outbound MTA Pipeline

The outbound pipeline also needs to be constructed with most effective and least resource intensive modules first. To control outbound electronic mail based on destination level of trust, the domain validation is performed early. In order to protect the destination electronic mail systems, SPAM and malware filtering are also performed early in the outbound pipeline.

The objective is to prevent the local enclave from forwarding any SPAM or malware issues. As an example, hosts in the agency enclave might be hijacked and included in a botnet like denial of service attack. By eliminating problematic electronic mail early, the more resource intensive content compliance and data loss prevention function will only process the minimum required messages.

The same rules identified in the outbound pipeline when identifying vendors for SPAM filtering modules. Based on the results of the pipeline functions, the outbound pipeline makes a mail disposition decision. The decision must be tunable based on agency policy. The available options are: reject to sender, redirect to a reviewer, or send. Since the sender is from inside the enclave, specific rejection conditions can be returned. The option of rejecting to a reviewer provides a mechanism to allow for human decisions. For example, the data loss prevention function might invoke the need for a human review. The send option permits the MTS to forward the message to the intended recipient. An important function of the outbound pipeline is to preserve the reputation of the agency when sending outbound messages.

The pipeline shows optional modules that can be plugged-in based on agency specific module. In Figure 4, the pluggable modules are annotated as optional and can be inserted as necessary. Any additional pluggable modules will be included as part of the agency specific module. For the outbound pipeline, all modules not marked as optional must be included. As with the inbound pipeline, outsourcing is possible but all modules must be accounted for in either the

outsourcing arrangements or by organic resources. For the mail disposition decision, the send and reject to sender options must be supported. The redirect to reviewer is optional based on specific agency policies.

3.2.2 Data Loss Prevention

Data Loss Prevention (DLP) is the most important functional module in the outbound MTA pipeline. It sequesters the transfer of sensitive information via an electronic mail message from the internal enclave to a lower-trust network. DLP products and solutions are still evolving in commercial off-the-shelf solutions and are designed to identify, monitor, and prevent the movement of sensitive information via electronic mail which can also help reduce insider threat or data exfiltration by malware and viruses.

DLP solutions must be able to scan electronic mail attachments as well as text regardless of whether it is encrypted. During the scanning, high risk data is identified and protected by means of sequestration. The challenge lies in reducing false positives while minimizing data leakage. As a result, federal agencies implementing DLP modules must be able to describe both the types and format of data requiring sequestration using both Bayesian logic and Unix-style regular expressions. The agency also needs to determine what actions must be taken once a violation is detected. As a result, the DLP process needs to be tightly linked to agency risk remediation policies and the selection of a specific DLP will also have implications as to how an MTA is configured.

3.2.3 Content Compliance

The content compliance module will look for electronic mail content in the outbound pipeline which does not comply with agency policies. In the context of the mail gateway architecture, content compliance is a decision based exclusively upon the types of content being distributed and not the actual content itself. For example, an agency policy might preclude sending attached images, video or executable files. The content compliance module looks at the file type not the content of the specific image and sequesters illegal content whereas the DLP module inspects otherwise legal content.

3.2.4 Malware Filtering

The malware filtering function is performed in both inbound and outbound MTA pipelines.

If the inbound MTA detects malware or viruses, the infected item must be moved into quarantine or deleted. In both cases, the event must be logged. The quarantined item could be the full message plus attachments or just the infected element. The location of the quarantine is not a function of the mail gateway architecture per se, but is a standalone application whose data is

supplied by the mail gateway architectures. Most implementations are done via web application or mail delivery agent modules.

For the outbound MTA, the malware filter module will send content to the reject processing decision handler. Agency rules will then determine if any components of the infected message are returned to the MUA or forwarded to the final destination with appropriate controls. In either case, the event must be logged and available to security administrators.

3.2.5 Domain Validation

Domain validation is performed by both the inbound and outbound MTA pipelines. This module determines the level of trust inherent to a given message sender's domain. This is accomplished using a combination of techniques ranging from black and white lists to SPF/DKIM records as well as the IP addresses of the mail originator.

Based on this status, an electronic mail message will be sent or modified according to agency policy. For example, if an untrusted sender domain is detected, the mail message may be returned to sender, dropped, or quarantined.

Domain Name System Security Extensions (DNSSEC), DomainKeys Identified Mail (DKIM), or Sender Policy Framework (SPF) extensions to the DNS can be used to validate domains and correlate them with IP addresses. If none of these technologies are implemented, a domain validating MTA may "fall back" to a simple white list or black list. In either case, domain validation will be critical to making other policy decisions regarding the delivery of mail.

3.2.6 SPAM Filtering

SPAM filters look for patterns in electronic mail and compare them with known and likely Spam signatures. The filtering techniques include a variety of approaches used in combination and are updated frequently. Electronic mail which is flagged as spam must be marked and either quarantined or deleted. Spam filtering is a critical component of the inbound MTA pipeline to reduce both denial of service (DoS) and phishing attacks and must evolve rapidly as commercial detection capabilities improve. This is a function which is commonly outsourced.

3.2.7 Agency Specific Modules

The provision of modular services along the inbound and outbound MTA architecture allows agencies to implement a variety of additional modules depending on agency policy or specific filtering requirements.

3.3 Security Requirements

3.3.1 Inbound Gateway Mail Transfer Agent (MTA) Requirements

In addition to high availability, an inbound MTA:

- Must include hot failover.
- Must be addressable by external networks (such as the public internet) and must be located in a network "demilitarized zone" (DMZ).
- Must support SMTPS transfers from outside domains opportunistically as well as unencrypted transfers from lower trust domains.
- Must be able to decode both Secure/Multipurpose Internet Mail Extensions (S/MIME) and/or Open Pretty Good Protection (OpenPGP) attachments.
- Must be able to query external DNS to obtain the SPF and/or DKIM key records associated with each incoming message.
- Must be able to verify DKIM signatures found on inbound electronic mail by querying external DNS information and verifying the cryptographic hash.
- Must be both fast and robust relative to the mail volume.
- Must be configured to deliver messages to one or more authorized internal mail delivery/transfer agents (MDAs/MTAs) as well as mail quarantine stores.
- Must be able to send SMTP mail to internal networks on port 25 in order to modularize mail-filtering transfer agents before finally delivering mail to user account mailboxes.
- Must be able to enforce agency specific security policies and be able to apply unique policies for individual source domains, permitting the mail transfer agent to enforce different security policies between federal organization, internet mail systems, or different enclaves.

3.3.2 Outbound Gateway Mail Transfer Agent (MTA) Requirements

In addition to appropriate capacity planning issues, an outbound MTA :

- Must be configurable to accept messages from one or more authorized internal mail submission agents (MSAs).
- Must be able to address external networks (such as the public internet) and therefore should also be located in an agencies DMZ.
- Must be configured to act exclusively as a relay for trusted MSAs and deny relay service to external mail systems.
- Must support the inclusion of RFC4871 compliant DKIM signature headers.

- Must be configurable to insert an RFC5322-compliant message header field to all outbound messages in its store and forward queue which encapsulates the RFC 1034 compliant domain name information of the sending/authorizing domain.
- Must be able to encode SDID public keys or obtain them from a local key server.
- Must support secure transactions with other network services including network time synchronization servers, data loss prevention tools and security log analysis tools such as network security event information managers (SEIMs).
- Must support transport layer security encryption via SMTPS for communication with capable recipients and be able to enforce agency specific security policies and be able to apply unique policies for individual destination domains.

3.3.3 Mail Submission Agent Requirements

MSAs must reside behind network firewalls and be configurable to forward all non-local mail to an outbound Mail Transfer Agent located either in the network DMZ or the inside perimeter firewall.

3.3.4 Mail Delivery Agent Requirements

Mail Delivery Agents receive mail from Mail Transfer Agents and therefore must be configurable to accept mail only from an inbound mail transfer agent and able to securely interact with local mail user agents (MUAs) over known ports via known protocols.

3.3.5 Mail User Agent Requirements

Mail User Agents (MUAs) must be able to:

- Create and pass on RFC compliant mail headers and must be configurable to support SMTP over port 587 for mail submission as specified in RFC 4409.
- Interact securely with agency directory servers and mail quarantine servers.

3.3.6 Domain Name System (DNS) Requirements

Because both DKIM and SPF depend upon the DNS system and neither provides intrinsic protection against spoofed DNS records, DNSSEC is needed to guarantee the validating records of the DNS. Therefore DNSSEC may be regarded as a pre-requisite for trusted mail identification on the internet, however the implementation of DKIM and SPF render email attacks more difficult even in the absence of DNSSEC secured DNS records.

In addition, external facing authoritative name servers must be able to:

- Respond to queries for DKIM public keys.
- Support the resolution of type 99 SPF records for all authorized outbound mail transfer agents within the agency administrative domain.
- Deliver RFC 4408-compliant Sender Policy Framework authorized mail server designations for all authorized mail transfer/exchange agents.
- Internal-facing authoritative name servers must be able to respond to queries for DKIM public keys.
- Internal recursive name servers must be able to issue recursive requests for DKIM and SPF compliant DNS records.

3.3.7 Firewall Requirements

Agency perimeter firewalls must be able to:

- Forward incoming SMTP mail on port 25 only to inbound MTAs.
- Block all other incoming ports from external networks directed to internal MTAs.
- Block all internal port 25 requests that do not originate from an MTA directed to an external server.
- Allow port 53 DNS recursion for outbound MTAs.
- Allow port 587 for internal mail submission.
- Based on agency policy, allow port 587 connections from MUAs originating from outside the enclave (it is strongly recommended this be prevented and a secure VPN connection be used instead).
- Allow port 80 or port 443 to the agency OCSP responder (the port is determined by the configuration of the OCSP server).
- Allow port 102 for the X.400 connector if external X.400 connections are required.

3.3.8 Logging Requirements

The mail gateway components must be able to:

- Gather and report statistical information for messages transferred inbound and outbound.
- Message logs must contain system health information, security policy violations, source and destination domain statistics, malware/virus detection and quarantine, server load levels, failures in mail gateway functionality, and DNS event errors.
- Comply with SEIM input queue requirements in accord with TIC Reference Architecture v2 logging functional requirement.

3.3.9 System Monitoring and Control

All mail gateway components must be able to:

- Log and send information to a security event information management system (SEIM).
- Minimum expected logging functions include Simple Network Management Protocol (SNMP) and/or Unix syslog functions but must also be configurable and extensible to meet specific risk profiles and electronic mail gateway control requirements and policies. The requirements for system monitoring and control need to be included in any outsourcing arrangement.

3.3.10 Archiving Requirements

- Inbound and outbound MTAs must provide archiving capability to align with agencies' electronic mail archiving policies (though archiving function can be satisfied by components outside the MTA pipeline).
- Individual agency policies determine if the MTA, MDA, MSA, and MUA should also archive the mail messages but the consolidation of those determinations into a formal archiving policy is imperative.
- MTAs do not perform an archiving storage function, but rather link to external archival systems.
- The MTA will host only internal log system logs. All other logs will be recorded and stored elsewhere (such as a network SEIM).

3.3.11 Audit Requirements

- In support of the federal and agency auditing requirements, the electronic mail gateway components must collect and provide access to auditing information.
- The transmission of transaction logs to external auditing systems must be either via electronic mechanism or human analysis of auditing, logging, and configuration data. This enables access to the information required to comply with FISMA and OMB security mandates.

4 Systemic Threats & Mitigations

A catalog of key threat types is listed in this section along with strategies for mitigating the threat type. See also RFC 4686.

Threat	Description	Impact	Mitigation

Denial of Service (DoS) attack against inbound MTA	DoS can be initiated intentionally either malicious attacker or unintentionally by a valid user/system.	Agency email can be disrupted or denied.	Hardened port firewalls should be combined with dedicated layer 7 firewalls to minimize DoS impact.
Denial of Service (DoS) attack against Key service	DoS can be initiated against DNS servers providing DKIM & SPF record information.	Agency email can be disrupted or denied.	DNS queries should be restricted to external nameservers; hardened port firewalls should be combined with dedicated layer 7 firewalls to protect DNS servers; inbound MTAs should use dedicated key serving resources.
Malware/virus infected mail message	Internal hosts can be compromised or rendered inoperable by malware passing through the email pipeline.	Any or all agency computing functions can be disrupted or denied.	Strict inbound mail filtering should be implemented using hardened appliances and/or third party services. Enclosures should be unpacked prior to delivery.
Malevolent hyperlink /"Phishing"	Internal hosts can be compromised or rendered inoperable by deceptive passing through the email pipeline which leads to the installation of malware or viruses.	Any or all agency computing functions can be disrupted or denied.	Strict inbound mail filtering should be implemented using hardened appliances and/or third party services. DNS blacklisting should be combined with link sequestration and proxy services to minimize threat.
Man-in-the-middle attack/	External upstream hosts are configured to queue mail for external domains from outside hosts.	Agency email can be disrupted, disclosed or denied.	Implement DNSSEC extensions and SPF framework to control MX record deployment *(See Appendix A).*

DNS Spoofing	Because both DKIM and SPF depend upon the DNS system and neither provides intrinsic protection against spoofed DNS records, DNSSEC is needed to guarantee the validating records of the DNS.	Agency email can be disrupted, disclosed or denied.	Implement DNSSEC extensions.
Unwanted electronic mail ("Spam")	Agency computing resources are wasted handling unwanted and unsolicited email.	User time is wasted and agency storage is wasted.	Establish rule-based mail filtering with real-time blacklist sensitivity; check for SPF and DKIM records from mail source.
Damaged or corrupted electronic mail	Mail is incorrectly transmitted to its destination due to failures in the MTA pipeline.	Agency email can be disrupted, disclosed or denied.	Closely monitor and log all MTA activity; apply vendor recommended patches and use message integrity checking where available.
Reputation Attacks	Forged outbound email may be used to damage the credibility or reputation of the agency.	Agency credibility is damaged.	Implement DNSSEC, DKIM and SPF extensions *(See Appendices A&B)*
Reflection Attacks	Intentionally mis-addressed messages are sent to third party MTAs, causing it to be "bounced" or sent to the return address on the message. The forged sender address then becomes the target of the "returned message".	Agency email can be disrupted or denied.	Establish rule-based mail filtering with real-time blacklist sensitivity; check for SPF and DKIM records from mail source and implement DKIM/SPF DNS extensions to prohibit return mail from outside sources *(See Appendices A&B)*

Theft of internal mail addresses	Recipient MTAs are tested for common names in order to identify targets for phishing attacks.	Sensitive agency information may be disclosed.	Do not return mail messages and provide only 500-series message fail notice; implement Bayesian anti-spam controls with real-time blacklist addition capability to discourage probing.
Verification Probe Attack	An extension of a mail probe is to send a message with a DKIM signature to many addresses without valid signatures and with a different selector. The attacker then monitors key service requests to determine which selectors had been accessed and which addressees used DKIM verification.	Sensitive agency information may be disclosed.	Place key servers behind firewalls and allow communication only with authorized hosts.
Relationship Exploitation	Forged email from familiar sender addresses is more likely to be acted upon by a recipient. Malware or spam may be delivered via this method.	Agency email can be disrupted, disclosed or denied.	Implement strict inbound mail filtering using hardened appliances and/or third party services. Enclosures should be unpacked prior to delivery and mail sources should be checked against SPF and DKIM records as well as real-time blacklists.

Signed message replay	Signed messages are retransmitted by an attacker to additional recipients beyond those intended by the original author. The attacker first receives a legitimate message from the victim and then retransmits it intact but with different envelope addresses in order to deliver unwanted email or malware.	Any or all agency computing functions can be disrupted or denied.	Implement both DKIM and SPF records along with DNSSEC extensions to prevent re-use of credentials from unauthorized sources *(See Appendices A&B).*
Chosen message replay	An attacker may create a message and obtain a valid signature by sending it through an MTA authorized by the originating domain. They then "replay" the signed message by sending it, using different envelope addresses, to a large number of other recipients.	Sensitive agency information may be disclosed.	Implement both DKIM and SPF records along with DNSSEC extensions to prevent re-use of credentials from unauthorized sources.
Packet Amplification Attacks	By requiring substantially larger DNS payload replies, DKIM contributes to denial-of-service attacks involving the transmission of spoofed UDP DNS requests to openly-accessible domain name in which the response from the name server is larger than the request, thereby forcing the name server to function as an amplifier for such an attack.	Agency email can be disrupted or denied.	Place public-facing DNS servers behind port firewalls using real-time blacklisting and stateful packet inspection; throttle responses based on service throughput.

False positives	Mail gateway incorrectly identifies legitimate mail as spam or malware.	Agency email can be disrupted, ignored or denied.	Implement spam quarantine inspection to facilitate manual spam validation.
Encryption weaknesses	Either weak or improperly configured encryption strategies are used.	Agency email can be compromised, corrupted, or source incorrectly identified.	Use FIPS certified encryption protocols whenever possible.

5 Security Configuration

Recommendation	Description	Key Benefits
Electronic mail gateways should be part of a unified mail-handling GSS under FISMA.	As an essential support system email should be consider holistically from a FISMA security standpoint.	More effective administration and monitoring of essential agency IT functions.
DNSSEC should be implemented prior to DKIM/SPF	Because both DKIM and SPF depend upon the DNS system and neither provides intrinsic protection against spoofed DNS records, DNSSEC is needed to guarantee the validating records of the DNS.	More robust and secure agency information services.
SPF rules should be implemented irrespective of DKIM as part of transition	Because SPF provides useful anti-spam capabilities that do not require strict identity establishment, it can be considered a useful transitional step forward to improving network identity services.	Better anti-spam/phishing controls.

6 Appendix A: Sample SPF Records

SPF domains have to publish at least two directives: a version identifier and a default mechanism. The simplest possible SPF record looks like the following:

```
agency.gov. TXT "v=spf1 -all"
```

This declaration means that *agency.gov* never sends mail. A domain which is only used for web services might have an SPF declaration such as this, but most domains will want to designate permitted hosts using one or more mechanisms.

If your MX servers send mail, you should designate them like this:

```
agency.gov. TXT "v=spf1 mx -all"
```

In this example, if *agency.gov* had an MX record, its MX servers would be designated as valid mail sources. If other machines in the domain also send mail, designate them as follows:

```
agency.gov. TXT "v=spf1 mx ptr -all"
```

This designates all the hosts whose PTR hostname match *agency.gov*. If any other machines not in the domain also send mail from that domain—such as, for example, a hosted mail solutions provider, designate them like this:

```
agency.gov. TXT "v=spf1 a:agency.gov mx ptr -all"
```

Each of your mail servers should have an SPF record also and consider creating an SPF record for every other machine in your domain.

Spammers can forge hostnames as well as domain names: to SMTP there is no difference between the two. If they start forging the hostnames of web servers, unix servers, even workstations, you'll want to create SPF records for those machines also.

If you send mail through another organization's servers, you should use an Include directive to point to their servers.

If other domains use exactly the same set of hosts, you can set up redirects for them. "Redirect" aliases point to other domains which themselves publish SPF records. This aliasing mechanism makes it possible to easily consolidate multiple domains that share the same set of designated hosts.

For more information see: http://www.openspf.org/

7 Appendix B: Sample DKIM domain record entry

DKIM is anti-spam/phishing method which works by signing outbound e-mail messages with a cryptographic signature which can be verified by the recipient to determine if the messages originate from an authorized system.

The process of signing outbound messages and verifying this signature is typically done by the e-mail servers at each end - not by end-users client software. DKIM uses DNS TXT-records to define policy and public encryption keys for a domain name.

The public key value is typically generated by a function in the e-mail server software or by using a tool such as "openssl". The public key must of course match the private key used by the e-mail server software to sign outgoing messages.

There are basically two types of DNS records used by DKIM; policy records and public key records.

Policy records:

A domain name using DKIM should have a single policy record configured.
This is a DNS TXT-record with the name "_domainkey" prefixed to the domain name - for example:

```
"_domainkey.agency.gov".
```

The simplest DKIM DNS entry looks like this:

```
sitename._domainkey.agency.gov IN TXT
"v=DKIM1; p=mypublickeygoeshere; s=email"
```

In this example, *sitename* is the name of the authorized mail transfer agent for *agency.gov* and the public portion of the domain key follows the p= designator.

The data of this TXT-record contains the policy which is basically either "o=-" or "o=~". "o=-" means "all e-mails from this domain are signed", and "o=~" means "some e-mails from this domain are signed". Additional fields for test (t), responsible e-mail address (r), and notes (n) may also be included - for example "o=-; n=some notes".

Receiving e-mail servers check this policy record to find out to what extent the sender domain name uses DKIM, if there is no such record, the domain does not support DKIM and it cannot be used to validate mail. Based on the stipulated policy, the receiving e-mail server might reject or flag un-signed messages from this domain name.

2) Public key records:

An e-mail message signed with DKIM will include a header item "DomainKey-Signature" containing the cryptographic signature and a few other fields including a "selector" (s=) - for example:

```
DomainKey-Signature: a=rsa-sha1;
s=sitename;
d=agency.gov;
c=simple;
q=dns;
b=dydVyOfAKCdLXdJOc8G2q8LoXSlEniSbav+yuU4zGffruD00lszZVoG4ZHRNiY
zR;
```

For the receiving e-mail server to verify this signature, it must first obtain the public key for the selector value. For above example, this is stored in a DNS TXT-record with the name "sitename._domainkey.agency.gov".

In other words, the name of this TXT-record is the selector (s=...) + ._domainkey. + the domain name.

The data of this TXT-record is in the format "k=rsa; p=MHww..." where value after p= is the public key. Additional fields for granularity (g), test (t), and notes (n) may also be included depending on individual requirements.

The selector value ("*sitename*" in above example) may be a fixed value used by your e-mail server software, or you may be able to configure multiple selectors for example for different branch offices or individual e-mail servers. The important thing is that for each selector used to sign outgoing messages from your domain name, you setup a separate TXT-record in DNS.

8 Appendix C: Acronyms – Common Abbreviations

BES – Blackberry Enterprise Server

CIO - Chief Information Officer

D/A - Department/Agency

DHS - Department of Homeland Security

DLP – Data Loss Prevention

DMZ – Demilitarized Zone

DKIM - DomainKeys Identified Mail

DNS - Domain Name System

DNSSEC - Domain Name System Security Extensions

DoS - Denial of Service

FIPS - Federal Information Processing Standards

FISMA - Federal Information Security Management Act

FNS - Federal Network Security Branch

IP - Internet Protocol

NIST - National Institute of Standards and Technology

NSTIC – National Strategy for Trusted Identities in Cyberspace

MTA – Mail Transfer Agent

MSA – Mail Submission Agent

MDA – Mail Delivery Agent

MUA – Mail User Agent

MX – Mail Exchange

OCSP – Online Certificate Status Protocol

OMB - Office of Management and Budget

PKI - Public Key Infrastructure

RFC – Request For Comment

SDID – Secure Digital Identification

S/MIME - Secure/Multipurpose Internet Mail Extensions

SEIMs - Security Event Information Managers

SPF - Sender Policy Framework

SMTP - Simple Mail Transfer Protocol

SMTPS – Simple Mail Transfer Protocol Secure

SNMP - Simple Network Management Protocol

TCP - Transmission Control Protocol

TIC - Trusted Internet Connections

UDP - User Datagram Protocol

UTA – User Transfer Agent

VPN – Virtual Private Network

9 Appendix D: Glossary – Common Terms and Definitions

Address Resolution Protocol (ARP) – A protocol used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the Internet Protocol (IP) address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted to it.

Body – The section of an email message that contains the actual content of the message.

Demilitarized Zone (DMZ): The DMZ (or Service Network) is a perimeter network segment that enforces the internal network information assurance policy for external information exchange.

Denial of Service (DoS): Intentionally or unintentionally overloading a computer resource to make a service unavailable.

Domain Name System (DNS): DNS is a hierarchical, distributed database for any resource connected to the Internet or private network that translates readable domain names to IP addresses.

Domain Name System Security Extensions (DNSSEC): DNSSEC is a suite of specifications that provides origin authentication, authenticated denial of existence, and data integrity to DNS clients (resolvers). DNSSEC was designed to prevent cache poisoning and does not provide services for availability or confidentiality.

Header – The section of an email message that contains vital information about the message, including origination date, sender, recipient(s), delivery path, subject, and format information. The header is generally left in clear text even when the body of the email message is encrypted.

Internet Message Access Protocol (IMAP) – A mailbox access protocol defined by IETF RFC 3501. IMAP is one of the most commonly used mailbox access protocols. IMAP offers a much wider command set than POP.

Intrusion Detection and Prevention System (IDS/IPS or IDPS): Identifies potential incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Local Delivery Agent (LDA) – A program running on a mail server that delivers messages between a sender and recipient if their mailboxes are both on the same mail server. An LDA may also process the message based on a predefined message filter before delivery. See also Mail Delivery Agent and Mail User Agent.

Mail Server – A host that stores incoming mail for distribution to users and forwards outgoing mail. The term may refer to just the application that performs this service, which can reside on a machine with other services, but for this document the term refers to the entire host including the mail server application, the host operating system and the supporting hardware.

Mail Server Administrator – The mail server equivalent of a system administrator. Mail server administrators are system architects responsible for the overall design and implementation of mail servers.

Mail Delivery Agent -- Mail Delivery Agents receive mail from Mail Transfer Agents

Mail Submission Agent – Mail Submission Agents forward all non-local mail to an outbound Mail Transfer Agent

Mail Transfer Agent (MTA) – A program running on a mail server that receives messages from mail user agents or other MTAs and either forwards them to another MTA or, if the recipient is on the MTA, delivers the message to the local delivery agent (LDA) for delivery to the recipient. Common MTAs include Microsoft Exchange and sendmail.

Mail User Agent (MUA) – A mail client application used by an end user to access a mail server to read, compose, and send email messages. Common MUAs include Microsoft Outlook and Mozilla Thunderbird.

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Multipurpose Internet Mail Extensions (MIME) – A protocol that makes use of the headers in an IETF RFC 2822 message to describe the structure of rich message content.

Network Administrator – A person who manages a network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

Open Pretty Good Privacy (OpenPGP) – A protocol defined in IETF RFCs 2440 and 3156 for encrypting messages and creating certificates using public key cryptography. Most mail clients do not support OpenPGP by default; instead, third-party plug-ins can be used in conjunction with the mail clients. OpenPGP uses a "web of trust" model for key management, which relies on users for management and control, making it unsuitable for medium to large implementations.

Operating System – The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its principal component, the kernel, resides in memory at all times. The operating system sets the standards for all application

programs (such as the mail server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.

Patch – An immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In many operating systems, a special program is provided to manage and track the installation of patches.

Phishing – Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Post Office Protocol (POP) – A mailbox access protocol defined by IETF RFC 1939. POP is one of the most commonly used mailbox access protocols.

Secure Multipurpose Internet Mail Extensions (S/MIME) – A protocol defined in IETF RFCs 3850 through 3852 and 2634 for encrypting messages and creating certificates using public key cryptography. S/MIME is supported by default installations of many popular mail clients. S/MIME uses a classic, hierarchical design based on certificate authorities for its key management, making it suitable for medium to large implementations.

Simple Mail Transfer Protocol (SMTP) – An MTA protocol defined by IETF RFC 2821. SMTP is the most commonly used MTA protocol.

Spam – Unsolicited bulk commercial email messages.

Spyware – Malware intended to violate a user's privacy.

System Administrator – A person who manages a computer system, including its operating system and applications. Responsibilities are similar to that of a network administrator.

Transmission Control Protocol (TCP): TCP provides reliable, ordered delivery of a stream of bytes on an Internet Protocol (IP) network from a program on one computer to another program on another computer. TCP, along with UDP, are the two core Network Protocols in the Internet Protocol Suite.

User Datagram Protocol (UDP): UDP allows computer applications to send messages (datagrams) to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP provides an unreliable service and datagrams may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. UDP, along with TCP, are the two core Network Protocols in the Internet Protocol Suite.

Vulnerability – A security exposure in an operating system or other system software or application software component. A variety of organizations maintain publicly accessible databases of vulnerabilities based on the version numbers of software. Each vulnerability can potentially compromise the system or network if exploited.

10 Appendix E: Selected Existing Guidance

10.1 LEGISLATION

E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

10.2 POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

National Security Presidential Directive (NSPD) 54, *Cyber Security and Monitoring*, 8 January 2008. Also known as HSPD-23.

Homeland Security Presidential Directive (HSPD) 23, *Computer Network Monitoring and Cyber-security*, 8 January, 2008. Also known as NSPD-54.

Office of Management and Budget (OMB) Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, 2 August 2005.

Office of Management and Budget (OMB) Memorandum *M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, 11 January 2007.

Office of Management and Budget (OMB) Memorandum M-08-05, *The Trusted Internet Connection initiative (TIC)*, November 2007.

National Security Telecommunications And Information Systems Security Committee NTTISSP 101, *National Policy on Securing Voice Communications,* 14 September 1999.

10.3 STANDARDS

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

General Services Administration (GSA), Public Buildings Service (PBS), *Facilities Standards (P100)*, 2009.

Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Module*, 3 December 2002.

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

Federal Information Processing Standard (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2006.

IEEE 802.1X: IEEE Standard for port-based Network Access Control (PNAC).

10.4 GUIDELINES

NIST's Information Technology Laboratory, ITL Security Bulletins, *An Introduction to Secure Telephone Terminals - ITL Security Bulletin*, March 1992.

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*, May 2010.

National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

National Institute of Standards and Technology Special Publication 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

National Institute of Standards and Technology Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009.

National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, June 2010.

National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

National Institute of Standards and Technology Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)*, December 2010.

National Institute of Standards and Technology Special Publication 800-81, Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, April 2010.

National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

Office of Management and Budget Memoranda, M-08-16, *Guidance for Trusted Internet Connection Statement of Capability Form (SOC)*, 4 April 2008.

Office of Management and Budget Memoranda, M-08-26, *Transition from FTS 2001 to NETWORX*, 28 August, 2008.

Office of Management and Budget Memoranda, M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*, 20 September 2008.

Office of Management and Budget Memoranda, M-09-32 *Update on the Trusted Internet Connections Initiative*, 17 September 2009.

Messaging Anti-Abuse Working Group, (MAAWG) Best Common Practices for Mitigating Abuse of Web Messaging Systems, August 2010

10.5 IETF RFCs

[Kohnfelder] Kohnfelder, L., "Towards a Practical Public-key Cryptosystem", May 1978.

[RFC0989] Linn, J. and IAB Privacy Task Force, "Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures", RFC 989, February 1987.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1113] Linn, J., "Privacy enhancement for Internet electronic mail: Part I - message encipherment and authentication procedures", RFC 1113, August 1989.

[RFC1848] Crocker, S., Galvin, J., Murphy, S., and N. Freed, "MIME Object Security Services", RFC 1848, October 1995.

[RFC1991] Atkins, D., Stallings, W., and P. Zimmermann, "PGP Message Exchange Formats", RFC 1991, August 1996.

[RFC2440] Callas, J., Donnerhacke, L., Finney, H., and R. Thayer, "OpenPGP Message Format", RFC 2440, November 1998.

[RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, August 2001.

[RFC3851] Ramsdell, B., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, July 2004.

[RFC4406] Lyon, J. and M. Wong, "Sender ID: Authenticating Electronic mail", RFC 4406, April 2006.

[RFC4407] Lyon, J., "Purported Responsible Address in Electronic mail Messages", RFC 4407, April 2006.

[RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in Electronic mail, Version 1", RFC 4408, April 2006.

[RFC4686] Fenton, J., "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)", RFC 4686, September 2006.

[RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

Attach 4

United States
Department of the Interior

Plan of Action and Milestones (POA&M) Process Standard Version 1.8

May 10, 2010

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
V1.0	05/04/2005	First release of document.	NA	NA
V2.0	05/13/2005	Bureau comments incorporated.	Various	Alan Wiser
V3.0	09/16/05	Revisions for clarification and to incorporate additional guidance regarding the relationship of POA&MS to Exhibit 300, Process Verification and POA&M Certification.	Various	Carole Dicker
V4.0	10/11/05	Final draft revisions for ITST comment and review.	Various	Larry Ruffin
V5.0	11/8/05	Revisions incorporating ITST comments.	Various	Larry Ruffin Carole Dicker
V6.0	12/5/05	Revisions incorporating additional ITST comments.	Various	Carole Dicker
V1.0	12/19/05	Revisions that incorporate FWS and BLM final comments.	Various	Carole Dicker
V1.1	02/09/06	Revisions that incorporate OSM final comments.	Various	Joe Seger
V1.2	02/09/06	Revisions that incorporate FWS final comments.	Various	Joe Seger
V1.3	12/20/06	Revisions incorporating the ITST's recommendation to add original weakness identification date to the master POA&M template.	Various	Jonas Manalansan
V1.4	01/30/07	Revisions and updates to POA&M reporting template.	Various	Andrea Yates
V1.5	01/28/08	Updated quarterly submission deadlines and points of contact.	Various	Davene Barton
V1.6	2/26/08	Revisions that incorporate ITST comments.	Various	Davene Barton

V1.7	3/19/10	The primary revisions incorporate CSAM Version 2.1.3, POA&M management enhancements (Section 4) to include procedures for re-creating POA&Ms that are closed inadvertently, a data field to identify the source of weakness and revisions to the Weakness Completion Verification Form (WCVF). The following documents were added as Appendices: OIG Recommendation Status Reporting Process, CSAM Account Management Procedures and CSAM Rules of Behavior.	Various	Davene Barton and William Ferrell
V1.8	5/10/10	Incorporated changes based on response to the OIG's "Verification of Previous Office of Inspector General Recommendations (Report No. ISD-EV-MOA-0002-2009)"	Various	Larry Ruffin

Table of Contents

1 INTRODUCTION 1
1.1 PURPOSE – ESTABLISH STANDARDS 1
1.2 BACKGROUND 1
1.3 SCOPE 1
2 GENERAL POA&M OVERVIEW 2
2.1 POA&M DEFINITION AND PURPOSE 2
2.2 THE POA&M IN CONTEXT OF CERTIFICATION AND ACCREDITATION 2
2.3 WHICH SYSTEMS REQUIRE A POA&M? 3
2.4 SYSTEM FUNDING AND BUDGETS 3
2.4.1 Funding 3
2.5 BENEFITS OF THE POA&M 4
2.6 ROLES AND RESPONSIBILITIES 5
2.6.1 Departmental Level 5
2.6.1.1 Chief Information Officer is responsible for: 5
2.6.1.2 Chief Information Security Officer is responsible for: 5
2.6.2 Bureau Level 5
2.6.2.1 Authorizing Official is responsible for: 5
2.6.2.2 Authorizing Official Designated Representative is responsible for: 6
2.6.2.3 Bureau Chief Information Security Officer is responsible for: 6
2.6.2.4 Chief Information Officer is responsible for: 7
2.6.2.5 System Owner is responsible for: 7
2.6.2.6 POA&M Coordinator is responsible for: 8
2.7 DEPARTMENTAL OVERSIGHT 8
2.8 HOW TO USE THE POA&M TO PRIORITIZE AND MANAGE REMEDIATION AND RISK 8
2.8.1 Prioritizing Weaknesses for Corrective Action 9
2.8.1.1 System Level Prioritization 9
2.8.1.2 Bureau Level Prioritization 9
2.8.2 Managing and Monitoring Progress 10
2.9 OVERVIEW OF THE POA&M REPORTING CYCLE 11
3 WEAKNESS REMEDIATION PROCESS 13
3.1 IDENTIFYING WEAKNESSES 13
3.1.1 Sources of Weaknesses 13
3.1.2 Including Weaknesses 14

3.1.2.1 Program Weaknesses 14
3.1.2.2 System Weaknesses 15
3.1.2.3 Weaknesses Identified Through an Office of Inspector General Evaluation 15
3.1.2.4 Weaknesses Identified Through Vulnerability Scanning and Penetration Tests 15
3.1.2.5 Weaknesses Identified Through The Incident Response Management Process 16
3.1.2.6 Weaknesses Identified Through The Internal Control Review Process 16
3.2 DETERMINE RISK IMPACT LEVEL 16
3.2.1 Weakness Risk Assessment 16
3.2.2 Risk-Based Exceptions 16
3.2.3 Documenting Accepted Risk 17
3.2.3.1 Prior to the system being placed into production: 17
3.2.3.2 After the accredited system is in the operational phase of its lifecycle: 17
3.3 DETERMINING CORRECTIVE ACTION PLAN OPTIONS 18
3.4 DETERMINING FUNDING AVAILABILITY 18
3.5 DETERMINING AN ESTIMATED COMPLETION DATE 19
3.6 DOCUMENTING THE CORRECTIVE ACTION PLAN IN THE POA&M 19
3.7 MONITORING AND REPORTING POA&M ACTIVITY 19
3.8 POA&M WEAKNESS COMPLETION PROCESS 19
3.8.1 Corrective Action Completion 20
3.8.2 Independent Verification of Corrective Action Completion 20
3.8.3 Bureau CIO Review of Corrective Action Completion 21
3.8.4 AO's Acknowledgement and Acceptance of Risk(s) 21
3.8.5 Documentation Updates 22
3.8.6 Weakness Completion Follow-Up 22
3.9 POA&M QUARTERLY CERTIFICATION TRANSMITTAL 22
4 CREATING AND MANAGING POA&MS 24
5 CONCLUSION 54
APPENDIX A: REFERENCES 1
APPENDIX B: ACRONYMS 1
APPENDIX C: GLOSSARY 1
APPENDIX D: WEAKNESS COMPLETION VERIFICATION FORM 1
COMPLETING CORRECTIVE ACTIONS 1
WEAKNESS COMPLETION VERIFICATION FORM 2
APPENDIX E: POA&M CERTIFICATION TRANSMITTAL 3
APPENDIX F: OFFICE OF INSPECTOR GENERAL RECOMMENDATION STATUS REPORTING PROCESS 1
APPENDIX G: CSAM ACCOUNT MANAGEMENT PROCEDURES 1

APPENDIX I: CSAM RULES OF BEHAVIOR I

List of Figures

Figure 1. Overview of POA&M Reporting 11
Figure 2. The POA&M Process for Weakness Remediation 13

List of Tables

Table 1. POA&M Dates and Deadlines 11

1 Introduction

1.1 Purpose – Establish Standards

The purpose of the *Plan of Action and Milestones (POA&M) Process Standard* is to provide Department of the Interior (DOI) personnel who have POA&M responsibilities with the standard procedures for developing, maintaining, and reporting their POA&M weaknesses in the Cyber Security Assessment and Management (CSAM) FISMA Reporting solution.

The *POA&M Process Standard* establishes the criteria for the POA&M process to ensure that bureaus and offices effectively implement DOI information technology (IT) security program requirements and that the DOI information security posture and program continues to improve.

1.2 Background

The *DOI POA&M Process Standard* incorporates the POA&M requirements mandated by the Office of Management and Budget (OMB) to comply with the *Federal Information Security Management Act of 2002* (FISMA). The Departmental Office of the Chief Information Officer (OCIO) has integrated the *POA&M Process Standard* into the DOI IT security program to formalize the process of remediating IT Security weaknesses, to ensure that weaknesses are appropriately prioritized for mitigation, and to ensure that all weaknesses are being addressed and resolved.

On April 30, 2007 Interior selected CSAM from the Department of Justice (DOJ), a Shared Services Center (SSC) under the OMB Information Systems Security Line of Business (ISS LOB) to automate FISMA data management and reporting for DOI.

CSAM provides DOI bureaus and offices with automated tools for managing security assessments, developing security plans, and reporting POA&M information. CSAM was purchased as Government Off-the-Shelf (GOTS) software from the DOJ, and during Quarter 4 of Fiscal Year 2008 all DOI bureaus and offices began to use CSAM to manage their FISMA-based information security programs.

1.3 Scope

This document applies to all DOI IT security programs and systems and those individuals having responsibility for:

- Management and operations of IT security programs and systems;
- Ensuring the effective security configuration and posture of systems;
- Identifying, documenting, and implementing corrective actions.

Any personnel tasked with completing POA&M activities should read this document to become familiar with POA&M standards and processes.

2 General POA&M Overview

A POA&M is a management tool that outlines identified IT security program and system weaknesses along with the tasks necessary to correct or mitigate them. To facilitate the remediation of weaknesses, the POA&M provides a means of planning and monitoring corrective actions; identifies those responsible for solving problems; assists in identifying security funding requirements; tracks and prioritizes resources; and informs senior management of the security status of programs and systems.

Remediation of security weaknesses is essential to achieving a mature and sound IT security program. A POA&M process to manage weaknesses is one of the key measures used by the Inspector General (IG), OMB, and Congress to assess an agency's information security program, posture and progress.

2.1 POA&M Definition and Purpose

The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and IT systems. DOI Program Managers are required to use POA&Ms to manage the activities needed to close their security performance gaps, assist the IG in his/her evaluation work of agency security performance, and assist with oversight responsibilities.

The POA&M presents an opportunity to highlight progress and demonstrate improvements in the quality and security of the IT security program. It is also designed to serve as a management tool and as a point of comparison for the OCIO in its assessment of the overall maturity of the DOI's IT security program status.

Though the POA&M is considered a comprehensive plan, OMB operates under the assumption that additional, more detailed project management plans exist for each corrective action item identified in the POA&M. It also assumes that the sources of identified weaknesses (e.g., IG audit reports and risk assessments) are readily available to provide original documentation of each weakness. Thus, each POA&M element should be clearly traceable to any additional project plans and back to its original source(s).

2.2 The POA&M in Context of Certification and Accreditation

According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 *Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*, the POA&M is a required document developed during the certification and accreditation (C&A) process and included in the final C&A package to document and help manage the mitigation of weaknesses identified during that process. The POA&M clearly informs the Authorizing Official (AO) of system weaknesses and their associated risks and presents their remediation plans or recommendation to accept the residual risk.

Once the AO authorizes a system for operation, the POA&M becomes part of the continuous monitoring process and is used to document and manage weaknesses identified throughout the system's lifecycle. POA&M weaknesses must be updated in CSAM no less than on a quarterly

basis. The OCIO Cyber Security Division (CSD) is responsible for reviewing and submitting quarterly reports to OMB in accordance with OMB instructions for preparing the FISMA report and Privacy Management report.

2.3 Which Systems Require a POA&M?

All systems that are either in the operational phase of their lifecycle or connected to a production environment potentially affecting other operational systems, or that process live production data require POA&Ms.[1] Below are some special circumstances, and the POA&M requirements they must meet.

POA&Ms ARE REQUIRED FOR:

- All systems in production in the operational phase of their lifecycle
- Systems connected to a production environment or processing production data (e.g. pilots), and
- Systems undergoing C&A in preparation for production environment.

- Systems undergoing C&A in preparation for entering a production environment require a POA&M as part of the C&A package. The C&A package POA&M identifies system weaknesses for which corrective actions have been planned and the required funding to implement the changes. New system POA&Ms are created prior to the first C&A phase (Initiation) and are added into CSAM at the time of their creation to ensure complete awareness of upcoming requirements.
- POA&Ms are no longer required for systems once they have been decommissioned.
- Typically, at least one POA&M should be maintained for each system[2]. Separate POA&Ms should not be submitted on minor applications or distributed segments of systems. Exceptions may include such circumstance as when there are instances of an application running locally such as FPPS.

2.4 System Funding and Budgets

2.4.1 Funding

POA&Ms are used by OMB to assess the state of the Federal Government's IT security and to aid in oversight of the Federal Government and its IT investments. OMB requires tying the POA&M to the budgeting process to ensure funding for IT security costs are considered throughout the system lifecycle. Systems that do not adequately address a plan for securing funding for mitigation of IT security weaknesses can be placed "at risk" and potentially lose funding.

---

[1] A production system is one that stores, transits or processes live data, or is operating in a production environment However, please note that if any system meets the described criteria, irrespective of whether or not it is considered to be a production system or in the operational phase of its life cycle (e.g., a pilot or development system either connected to a production environment or that processes production data/information) requires either have an Interim Approval to Operate (IATO) or Authorization to Operate (ATO) and appropriate C&A documentation, including a POA&M.

[2] A system is defined by the accreditation boundary as documented in the C&A package's System Security Plan (SSP). The inventory of systems must also be maintained in CSAM by each bureau or office and there must be a POA&M corresponding to each of those systems.

For major investments, OMB requires that POA&Ms be cross-referenced through answers to questions when completing section II.B. of the Exhibit 300. The response to all questions in this section of the Exhibit 300 should align with weaknesses reported in the POA&M. Answers to question II.B.1 (A) in the Exhibit 300 *("What is the total dollar amount allocated to IT security for this investment? Please indicate whether an increase in IT security funding is requested to remedy IT security weaknesses, specifying the amount and a general description of the weakness.")* should link to each system-level POA&M weakness in the following manner:

- Although the total dollar amount allocated to IT security for the system may not match the POA&M exactly, the Exhibit 300 will include figures from the POA&M in addition to security costs as a separate, but related, component of the ongoing operational and maintenance (O&M) costs.
- The increase in security funding necessary to mitigate the weakness should match those listed in the "Cost" field of the POA&M.
- Identification of the security weaknesses noted in the capital planning document should match those identified in the POA&M.

Bureau or office system owners and Chief Information Officers (CIOs) are responsible for ensuring that the IT security costs necessary to remediate weaknesses are identified, reviewed, and considered in the bureau or office Capital Planning and Investment Control (CPIC) processes, and clearly identified in the POA&M and the Exhibit 300s in a manner that easily distinguishes those costs from routine IT security related O&M costs.

2.5 Benefits of the POA&M

Through the process of strategically addressing vulnerabilities and weaknesses in the POA&M, the mission of DOI can proceed without interruption or failure in appropriate delivery. Beyond its function as the primary authoritative IT security management tool for addressing weaknesses, the POA&M has other benefits related to producing valuable information for trending and analysis, which supports IT business cases, and helps to maintain institutional knowledge and facilitate effective communication among relevant system personnel. Each of these uses provides the OCIO with greater control over its IT security program and increases the efficiency of IT security management.

- **Producing Trending and Analysis Information.** The POA&M can be used as a historical data source for management reporting and business intelligence on the costs, effort, and time to mitigate IT security weaknesses. The type of weaknesses occurring can be tracked, as well as their rate of recurrence. The POA&M provides the ability to conduct analyses by system, program, or across the DOI enterprise.
- **Supporting Business Cases.** A comprehensive POA&M with accurate and reliable financial estimates provides traceability and documents the security funding needed to mitigate weaknesses, specifically at the operational phase of the system lifecycle.
- **Maintaining Institutional Knowledge.** A mature POA&M prevents reliance on one individual to retain and communicate information pertinent to a system or an entire program.

- **Facilitating Effective Communication.** The POA&M facilities communication and coordination among personnel, such as the CIO, system owners/managers, budget personnel, and program officials.

2.6 Roles and Responsibilities

Within DOI and across the Federal Government, many job roles include POA&M responsibilities. This is because POA&Ms are designed to be used by various types of personnel, including CIOs, Bureau Chief Information Security Officers (BCISOs), the IG, program officials, system owners and system managers, to track the progress of corrective actions for an IT system's weaknesses.

OMB's guidance directs CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems that they operate and control. For example, for program officials, this includes all systems that support their operations and assets. While much of the focus of security involves IT security professionals, collaboration should also occur with senior management to ensure that weakness mitigation plans are in alignment with the organizational mission and that funding is allocated appropriately. Coordination with budget and program personnel then ensures that weakness mitigation funding is incorporated into capital planning where necessary.

The following DOI role descriptions identify the POA&M responsibilities of each. It is recognized that there may be other individuals with varying titles throughout the bureaus and offices that have been delegated responsibility to fulfill some of the described roles.

2.6.1 Departmental Level

2.6.1.1 Chief Information Officer is responsible for:

- Reporting to OMB on agency progress related to correcting weaknesses reflected in the POA&M and the results of independent IG inspections;
- Reviewing the quarterly POA&M and ensuring that bureaus and offices have followed policies and procedures when completing their respective POA&Ms.

2.6.1.2 Chief Information Security Officer is responsible for:

- Reviewing bureau- and office-level POA&Ms, ensuring that the POA&Ms comply with Department-wide and OMB guidance;
- Implementing a quality assurance process that ensures all systems in the bureau or office system inventory are accounted for, that weaknesses are adequately described, and that planned corrective actions appropriately address the weaknesses.

2.6.2 Bureau Level

2.6.2.1 Authorizing Official is responsible for:

- The quarterly review of systems under their purview prior to the submission of POA&Ms for OMB reporting;
- Reviewing all residual risk(s) recommended for acceptance by the System Owner, User Representative, System Manager, or BCISO.

The Authorizing Official (AO) must either approve or reject each recommendation for risk acceptance. This is an extension of the AO's role of accepting or rejecting risk in the issuance of an authorization to operate (ATO). The AO may delegate activities surrounding the POA&M, but cannot delegate the acceptance of risk to the agency[3] and must therefore be the direct approver of any residual risk.

Because of the breadth of organizational responsibilities and significant demands on time, an authorizing official cannot always be expected to participate directly in the planning and technical meetings that occur during the POA&M management process. The AO's designated representative is an individual acting on the authorizing official's behalf in coordinating and carrying out the necessary activities required during the POA&M management and remediation process for an information system.

The AO's designated representative can be empowered by the authorizing official to make certain decisions with regard to the planning and resourcing of the remediation activities associated with weaknesses identified on the POA&M and the determination (but not acceptance) of risk to agency operations, assets, and individuals.

The only activity that cannot be delegated to the AO's designated representative is the acceptance of risk and signing of documents in which the AO indicates acceptance of risk to the agency or IT systems and associated information.

2.6.2.2 Authorizing Official Designated Representative is responsible for:

- Interacting with the BCISO, Information System Owners, System Security Managers, User Representative(s), and other interested parties during the POA&M management and remediation process;
- Reviewing the quarterly POA&Ms and obtain the authorizing official's signature on acceptance of any residual risks when called upon.

If an AO's designated representative is not selected, the AO is responsible for carrying out the activities described above.

2.6.2.3 Bureau Chief Information Security Officer is responsible for:

- Managing the POA&M process to include collection and consolidation of POA&M weaknesses at the bureau level for departmental reporting;
- Ensuring that all OIG recommendations have a corresponding POA&M weakness created in CSAM;
- Communicating standards and procedures related to the POA&M process;
- Reviewing POA&M weakness descriptions to ensure that they adequately describe identified weakness;
- Reviewing corrective actions to ensure that each is an effective and appropriate mitigation solution for its targeted weakness;

[3] Refer to NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Page 35.

- Reviewing milestones to ensure that they are relevant and will result in correction or mitigation of each weakness;
- Ensuring that all supporting evidentiary artifacts that support closure of a POA&M weakness has been uploaded into CSAM as an artifact to include, but not limited to, Weakness Completion Verification Forms (WCVFs, screenshots and policy-related documents;
- Reviewing all accepted risk recommendations, ensuring that appropriate justifications are provided and adequately explained;
- Formulating the recommended bureau priority level for identified weaknesses in consultation with System Owners;
- Verifying the completion status of system security weaknesses reported in POA&M;
- Providing routine review and status reports on corrective actions to the bureau CIO, no less than quarterly.

2.6.2.4 Chief Information Officer is responsible for:

- Performing reviews of quarterly POA&M weaknesses and ensuring the accuracy and completeness of the reports;
- Reviewing resource and funding requirements to ensure adequate funding has been identified and committed to implement corrective actions for each weakness;
- Reviewing and reassessing the prioritization of corrective actions;
- Reviewing corrective action verifications to confirm adequate testing and independent review;
- Certifying completed corrective actions in preparation for submission of the FISMA quarterly report, thereby ensuring that completed security weakness remediation activities are documented;
- Ensuring that appropriate program officials have reviewed and accepted any residual risks no less than quarterly.

2.6.2.5 System Owner is responsible for:

- Developing, managing, and implementing POA&Ms;
- Ensuring corrective actions are implemented in a timely manner consistent with the scheduled commitments to resolve weaknesses as documented on their POA&M;
- Preparing documentation for verification of completed POA&M items;
- Completing and uploading Weakness Completion Verification Forms (WCVF) into CSAM as artifacts prior to closing POA&Ms;
- Uploading evidentiary artifacts into CSAM in all updates whether the POA&M remains open or is closed to demonstrate progress in remediating weaknesses;
- Completing and uploading Bureau CIO POA&M Certification Transmittal memoranda into CSAM;

- Updating the C&A package with documentation on completed POA&M items (append approved verification form);
- Conducting a routine review and ensuring that updates are entered into CSAM to reflect corrective actions no less than quarterly, in coordination with the BCISO.

2.6.2.6 POA&M Coordinator is responsible for:

The POA&M coordinator is responsible for collecting updated POA&M and or POA&M data from the System Owners or their designees.

- Entering into CSAM POA&M weaknesses and/or updated POA&M weakness information from the System Owners or their designees;
- Ensuring that all supporting evidentiary artifacts that support closure of a POA&M weakness has been uploaded into CSAM as an artifact to include, but not limited to, Weakness Completion Verification Forms (WCVFs, screenshots and policy-related documents;
- Consolidating POA&Ms for quarterly submission to the Cyber Security Division (CSD).

2.7 Departmental Oversight

The Department Manual, part 18, paragraph 18.5(A)1, requires CSD to perform "oversight." In addition, part 375, chapter 19, paragraph 19.8(D)10, requires the Department's CISO to oversee "bureau compliance with Federal and Departmental policies, guidelines, and regulations governing IT security."

The *POA&M Process Standard* establishes the criteria for implementation of DOI's POA&M process as mandated by OMB. DOI's OCIO CSD is responsible for ensuring that POA&Ms meet established criteria and are effective in prioritizing and managing weakness remediation and meeting their ultimate purpose of continuously improving the security posture of IT programs and systems throughout DOI. In the event POA&M weakness entries are not in compliance with the *POA&M Process Standard*, the CSD will issue corrective action recommendations to the respective bureau/office POA&M Coordinator.

The CSD will perform annual independent compliance inspections of a sample of completed POA&M corrective actions and will provide reports on the effectiveness of the POA&M processes within each bureau and office.

Each bureau and office should consider the effectiveness of their internal control processes and implement similar verification and validation processes to maintain the integrity of their POA&M and weakness remediation processes. Verification and validation processes should be administered by individuals other than those who are actually responsible for implementing the corrective actions.

2.8 How To Use the POA&M To Prioritize and Manage Remediation and Risk

The POA&M provides a standard format for viewing identified weaknesses and the necessary information to prioritize and manage remediation efforts.

2.8.1 Prioritizing Weaknesses for Corrective Action

FISMA guidance requires Federal agencies to prioritize weaknesses within POA&Ms to help ensure that significant IT security weaknesses within POA&Ms take precedence.

The funding and personnel resources necessary to remediate every weakness identified in the POA&M may not always become available. Therefore, by prioritizing weaknesses in consideration of the varying risk levels associated with each weakness, the bureaus can ensure that critical and high-priority weaknesses receive the funding and personnel resources necessary to complete corrective actions.

The most critical weaknesses for the most critical systems must be considered first. It is not expected, however, that weaknesses will always be resolved in order of severity. Some will require longer-term planning, reallocation of Bureau and Departmental resources, or additional funding. It also often makes sense to resolve the weaknesses that require little effort and use existing funding regardless of priority or weakness severity, assuming the effort does not detract from the more critical issues.

2.8.1.1 System Level Prioritization

At the system level, criteria to be considered in prioritizing weaknesses for corrective action include:

- Risk impact level of weakness (CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level. The criticality value is dynamically updated as the associated control implementation status changes);
- Resource (funding and staff) availability;
- Level of effort required to complete corrective action;
- Cost benefit of corrective action (See NIST SP 800-30 for recommendations in performing cost-benefit analysis);
- Length of time since the weakness was identified;
- The AO's tolerance for the duration of risk exposure;
- Circumstances unique to the system.

Program officials and System Owners in consultation with the BCISOs should use their best judgment in consideration of the above factors and incorporate the urgency for corrective actions into their project plans.

2.8.1.2 Bureau Level Prioritization

At the bureau level, prioritizing weaknesses for corrective action is necessary for an effective allocation and/or reallocation of funds. Prioritizing weaknesses for corrective action is more complicated than it is at the system level, as the decision must consider all of the bureau's systems. The following factors should be considered at the bureau level:

- The security categorization of the system as defined by the NIST Federal Information Processing Standard (FIPS) Publication (Pub) 199[4] and the associated potential impact ratings for confidentiality, integrity, and availability. This is documented in each system's System Security Plan (SSP). Prioritization of corrective actions should be based on the most critical and sensitive systems first;
- The risk impact level of each weakness within a system's POA&M;
- Potential corrective action cost;
- Cost/benefit of corrective action;
- Potential for funding reallocation;
- Extent of the system's overall non-compliance.

Although a formal cost/benefit analysis is not required, for large systems with potentially costly corrective requirements, good project management may call for a cost benefit analysis to determine the best solution and acceptable level of residual risk.

2.8.2 Managing and Monitoring Progress

The POA&M is intended to serve as a tool for managing the progress of corrective actions and thereby managing risk posed by the weaknesses. At all levels—system, bureau, OIG, Departmental—the POA&M provides a view of progress within each system, for the system as a whole, and on a bureau-wide level.

Individual POA&Ms should be reviewed regularly to determine whether there are unnecessary delays, if priorities have shifted in light of newly identified weaknesses or environmental changes, and whether resources need to be re-evaluated. At the bureau level, the System Owner and BCISO are tasked with this responsibility, but it is also within the purview of the CIO to provide oversight. From a wider perspective, common weaknesses across the bureau or agency can be detected and more effectively dealt with, or areas requiring additional attention can be identified.

The quarterly reporting schedule for bureaus and offices to have POA&M updates entered into CSAM is depicted in the table below. Please note that if the due date falls on a Saturday or Sunday the updates are due the following Monday by close of business.

[4] System security categorization should be determined according to the criteria articulated in the Federal Information Processing Standards (FIPS) Publication 199, *Security Categorization of Federal Information and Information Systems* and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems.*

Quarter	Time Period Covered	Deadline for bureaus and offices to have updates entered into CSAM	Deadline for CSD Submission of Report to OMB
1st	Aug 1 - Oct 31	November 6	December 1
2nd	Nov 1 – Jan 31	February 6	March 1
3rd	Feb 1 – Apr 30	May 6	June 1
4th	May 1 – Jul 31	August 6	September 1

Table 1. POA&M Dates and Deadlines

In summary, the POA&M provides a means to monitor corrective actions, to ensure flexibility as the environment changes, to maintain a focus on priorities, and to minimize delays. It facilitates the decision-making process with regard to budget formulation and resource allocation or re-allocation. The POA&M is also a means to demonstrate compliance with policy and to show progress toward an improved security posture.

2.9 Overview of the POA&M Reporting Cycle

OMB POA&M reports consist of summary information on identified weaknesses, which are tracked in the agency's program and system POA&Ms. POA&M reports that are broken down by major agency components--DOI bureaus and offices--must be submitted quarterly to OMB.

DOI bureaus and offices are the source of this information, and must therefore provide the DOI CSD with up-to-date POA&M packages via CSAM on a quarterly basis. The DOI CSD program office then reviews and consolidates the information and presents the quarterly report to the Departmental CIO. The Departmental CIO reviews and approves the report and forwards it on to OMB.

The quarterly POA&Ms provide OMB with a 'snapshot in time' of the ongoing activity directed toward improving DOI's overall IT security posture.

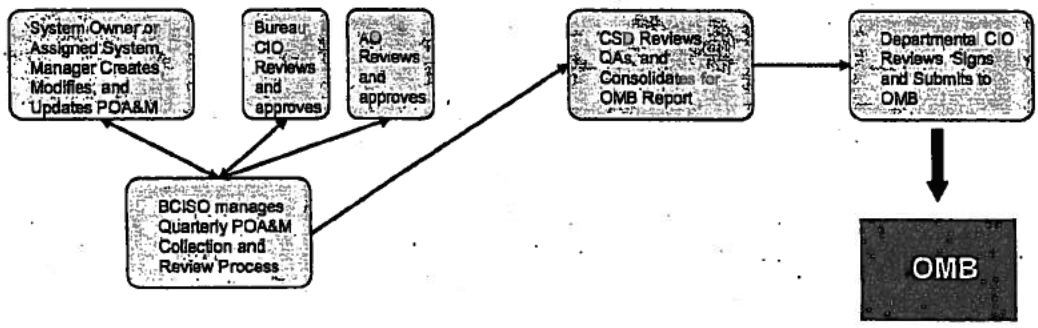


Figure 1. Overview of POA&M Reporting

Bureaus and offices should establish their own internal deadlines consistent with the time period covered and CSD's deadline for POA&M package submission to OMB. In order to meet the

regularly occurring deadlines, it is recommended that System Owners – or individuals delegated the POA&M responsibility—integrate the POA&M process into a continuous monitoring process. This will allow for sufficient time to gather information, make certain decisions, and obtain necessary AO and CIO quarterly review and approval. Each bureau or office POA&M update must include:

- **Updated POA&M for each system** in the bureau or office inventory and the bureau or office IT security program. (See Section 2.3, *Which systems require a POA&M?*) For each system and program the POA&M weakness must be updated in CSAM no less than quarterly to include updates to all relevant date fields as well as key milestones.

The key milestones associated with each corrective action should be identified on each POA&M. Each weakness must have one or more associated milestones. Milestones should define the major steps that will be performed to complete the corrective action. If there is more than one milestone, enter the milestone in the order they should be executed. For example, one set of milestones for a weakness such as, "Identification and authentication are not adequate for the level of security controls required for this system" might be:

1) Evaluate methods for strengthening identification and authentication.
2) Recommend solution and obtain approval.
3) Develop procedures to standardize accepted identification and authentication process.
4) Design identification and authentication solution.
5) Build identification and authentication solution.
6) Test identification and authentication solution.
7) Deploy identification and authentication solution and implement supporting process.

Milestones might also include more specific aspects related to the technical solution (e.g. implement two-factor authentication), and management and operational controls related to the steps for implementing supporting business practices and procedures where additional security control requirements are known or anticipated.

The description of each milestone must be detailed enough so that an independent reviewer will understand the planned corrective action and determine whether the corrective action is adequate and appropriate and will result in the weakness being corrected or its associated risk mitigated to a level acceptable to the AO. The last milestone entry must clearly identify the action taken to mitigate the weakness. Sensitive information can be included as needed for the description since the entire POA&M is a sensitive but unclassified document.

A copy of the WCVF for each system which will be uploaded as an artifact into CSAM. Each completed weakness requires a form, signed by the System Owner, an Independent Reviewer, Lead Responder, the CIO, and the AO if there is any residual risk. (See Appendix D, *Weakness Completion Verification Form.*)

- **POA&M Certification Transmittals,** signed by the bureau or office CIO covering all systems within his or her respective bureau or office. The transmittal certifies that the POA&Ms were completed in accordance with DOI OCIO Directive 2006-007. The CIO Certification Transmittal must list each system in the bureau or office inventory, its

operational status (pre-production, production, or decommissioned), and its C&A status (ATO, IATO, no authorization to operate). (See Appendix E, *POA&M Certification Transmittal.*)

Attached to each CIO Certification Transmittal are the **AO Certification Transmittals** indicating review of the POA&Ms for the systems for which each AO is responsible. (See Appendix E, *POA&M Certification Transmittal.*)

3 Weakness Remediation Process

Weakness remediation consists of a cycle that entails the steps depicted in Figure 2 below.

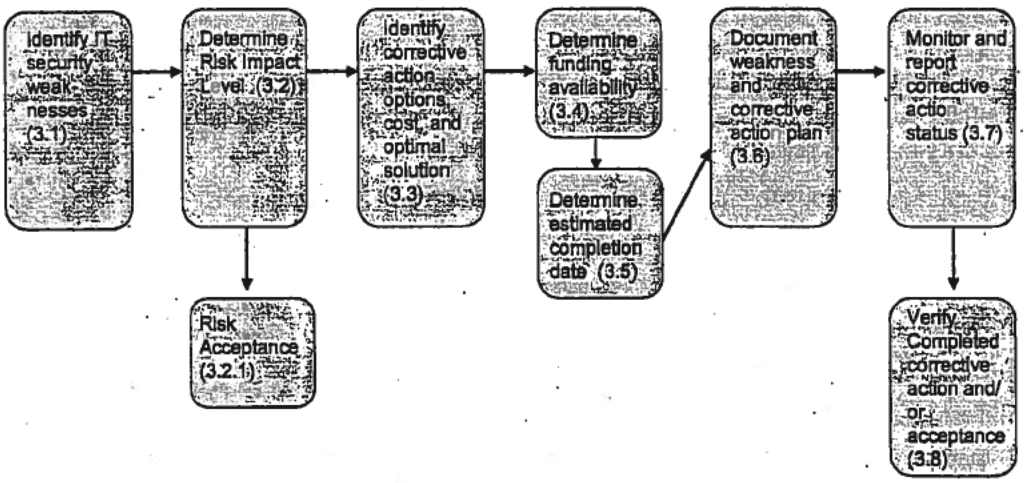


Figure 2. The POA&M Process for Weakness Remediation

This section describes the Weakness Remediation Process for implementing the steps in this process, including the identification, documentation, and updating of weakness information in the POA&M. Section 4 provides instructions for recording all required information into CSAM, including a field-by-field description of the POA&M contents.

3.1 Identifying Weaknesses

Weaknesses to be recorded and tracked through the POA&M process can be identified through either reactive or proactive processes. Reactive weakness determination indicates that outside auditors or reviewers identified the weakness. Proactive weakness determination occurs by conducting regular program and system reviews using various internal assessments.

3.1.1 Sources of Weaknesses

A DOI-specific User Defined Attribute (UDA) labeled "Source of Weakness" has been created within CSAM and is now an attribute of every POA&M weakness. This is in addition to the existing DOI-specific UDA labeled as "Created as a Result of an OIG Evaluation" having a value of either "Yes" of "No" that will continue to be maintained to enable the OIG to more efficiently identify all POA&M weaknesses that are associated with OIG report findings and

recommendations. The new "Source of Weakness" UDA provides a text field with a sufficient number and types of permissible characters for bureaus/offices to identify all sources of weaknesses by including the auditing entity, the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.

Typical sources of identified weaknesses that must be added to the POA&M include, but are not limited to, the following:

- OIG audits and reviews
- OCIO - FISMA activities
- Annual self-assessments
- GAO reviews
- Court ordered reviews
- OMB activities
- Third party audits
- Risk assessments
- Penetration tests
- Vulnerability scans
- Day-to-day operations

Bureaus/Offices must enter the source of each weakness and must include the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.

3.1.2 Including Weaknesses

POA&Ms must include all security weaknesses, not just material or reportable weaknesses, associated with DOI systems and programs. Weaknesses that can be corrected in a short time frame or are considered low risk and acceptable must still be included in the POA&M and tracked until verified as complete. The POA&M is the authoritative DOI-wide management tool and, as such, should represent an all-inclusive view of identified security weaknesses. The two types of weaknesses, program and system, are described below.

3.1.2.1 Program Weaknesses

A program weakness impacts multiple IT systems as a result of a deficiency in the IT security program. Program weaknesses are generally weaknesses that affect the bureau or office as a whole. Program weaknesses are addressed separately from individual system weaknesses. An example of a program weakness is: "Security policy is not updated with latest legislative guidance."

3.1.2.2 System Weaknesses

A system weakness pertains to the management, operational, or technical security controls of a specific IT system. Each set of system-specific weaknesses is noted under separate headers in a POA&M. An example of a system weakness is: "System has not been certified and accredited/authorized to operate."

3.1.2.3 Weaknesses Identified Through an Office of Inspector General Evaluation

All weaknesses identified as a result of an OIG evaluation should have a single unique POA&M weakness created for each individual recommendation within three business days of receiving the report. (See Appendix F, *Office of Inspector General Recommendation Status Reporting Process.*) In other words, there should only be a single POA&M item per OIG recommendation, even if the corrective action for each appear to be the same. This requirement stems from a previous OIG finding and recommendation and currently only applies to OIG recommendations.

3.1.2.4 Weaknesses Identified Through Vulnerability Scanning and Penetration Tests

Weaknesses may be identified during routine vulnerability scanning (e.g., weekly or monthly) in support of the continuous monitoring process. These vulnerabilities should be validated and the POA&M weakness must be created in CSAM. It is recognized that there may be false positives and that a number of weaknesses may be immediately resolved. There are also varying levels of risk for the vulnerabilities identified in the scans. The following discussion addresses guidelines regarding pre-POA&M evaluation.

Pre-POA&M Evaluation and Corrective Action –The following guidelines should be used to prioritize, evaluate, and validate the scanning results.

- High-risk or critical vulnerabilities associated with internet-accessible and/or externally facing systems have a period of up to ten (10) calendar days prior to recording weaknesses as a POA&M in CSAM. (Note, however, that such vulnerabilities are typically associated with any attacker being able to exploit a weakness remotely without requiring elevated/privileged access to a system and should be addressed immediately by disabling any access to the vulnerable service until the risk can be mitigated to at least a medium level before restoring the service);
- Medium-risk vulnerabilities associated with internet-accessible and/or externally facing systems have a period of up to thirty (30) calendar days prior to recording weaknesses in a POA&M;
- Low-risk vulnerabilities associated with internet-accessible and/or externally facing systems have a period of up to sixty (60) calendar days prior to recording weaknesses in a POA&M;
- High-risk vulnerabilities associated with internal systems (that are NOT internet-accessible and/or externally facing) have a period of up to fifteen (15) calendar days prior to recording weaknesses in a POA&M;
- Medium-risk vulnerabilities associated with internal systems (that are NOT internet-accessible and/or externally facing) have a period of up to thirty (30) calendar days prior to recording weaknesses in a POA&M;

- Low-risk vulnerabilities associated with internal systems (that are NOT internet-accessible and/or externally facing) have a period of up to sixty (60) calendar days prior to recording weaknesses in a POA&M;

Aggregating Scan Identified Vulnerabilities Into Individual POA&Ms – Multiple vulnerabilities from a vulnerability scan or any other source cannot be recorded as a single POA&M weakness entry. Each vulnerability or weakness identified should be verified and an individual POA&M weakness must be created for each weakness. The source of the weakness must be identified in the "POA&M Title" field within CSAM.

3.1.2.5 Weaknesses Identified Through The Incident Response Management Process

Weaknesses identified through the Incident Response Management Process should typically be included in a POA&M. However, if remediation is completed immediately as part of the incident response, if the DOI-CIRC incident report sufficiently documents the corrective action, and if the corrective action fully addresses the weakness (e.g., there is no resulting residual risk), then it is not necessary to report it as a POA&M or in an existing POA&M. A POA&M entry is required if corrective action is not completed within five (5) calendar days.

3.1.2.6 Weaknesses Identified Through The Internal Control Review Process

Weaknesses identified through the Internal Control Review (ICR) process must be entered into CSAM as part of the documentation process. A copy of the POA&M is **not** required as part of the ICR submission. A POA&M weakness must be created in CSAM with identified corrective measures necessary to bring each security control into full compliance, unless a prior POA&M weakness was created and the risk has been accepted or compensating controls are in place.

Bureaus and offices must submit within their assurance statements, as part of their normal POA&M reporting process, all weaknesses that note a deficiency of security controls for their information systems. POA&M submissions of the weaknesses identified during the ICR process are required regardless of whether their conditions rise to the level of being "reportable."

3.2 Determine Risk Impact Level

3.2.1 Weakness Risk Assessment

CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level. The Criticality value is dynamically updated as the associated control implementation status changes.

3.2.2 Risk-Based Exceptions

In some cases, a specific corrective action may not exist for a weakness because the weakness is considered an acceptable risk. The weakness must still be recorded in the POA&M to document the decision in the quarter in which it was discovered and must continue to be reported until the risk is formally accepted by the AO. The AO is the only official that has the authority to accept the residual risk from a partially or un-remediated weakness.

The AO acknowledges and accepts the risk when he or she completes the quarterly review of the POA&M containing the documented weakness. At a minimum, the CIO, System Owner, System Manager and/or BCISO should provide the AO with a quarterly briefing of the information

necessary for the AO to make an informed, risk-based decision regarding the POA&M-defined milestones with respect to accepting the existing residual risks.

All high-risk weaknesses must be corrected if possible or otherwise mitigated to at least a medium level of risk. (The AO can only consider acceptance of medium or low risks) Every effort must be made to correct or further mitigate all risks to a level commensurate with the potential impact to systems and associated data.

3.2.3 Documenting Accepted Risk

Using the WCVF (Appendix D), and complying with an approved procedure to assess risk such as that identified in NIST 800-30, *Risk Management Guide for Information Technology* the System Owner or designated individual should record the rationale and justification for risk acceptance to facilitate the AO's decision-making process. The System Owner should take measures to fully understand and document the level of risk and possible compensating controls. Measures such as researching the risk and evaluating industry common best practices for remediation strategies will show the System Owners prudent judgment and due diligence. Because risks can change over time, the System Owner should also periodically review the system's accepted risks to assess any potential changes in the acceptable risk level. Details on the process and documentation for acceptance of risks are further discussed in Section 3.8, *POA&M Weakness Completion Process*.

The AO's risk acceptance must also be appropriately documented. The following scenarios are acceptable forms of documenting risk acceptance decisions. Rationales and justifications must be included in the documentation.

3.2.3.1 Prior to the system being placed into production:

At the time the AO issues an ATO for a specific system, risks to be accepted by the AO can be documented in either the:

- The AO's Accreditation Memorandum;
- The Certifying Official's Certification Statement with a reference in the AO's Accreditation Memorandum stating that the risks identified in the Certification Statement are to be accepted; or
- The SSP with a statement in the AO's Accreditation Memorandum stating that the risks identified in the SSP are to be accepted.

The Accreditation Memorandum should also include an explicit statement that the AO acknowledges and accepts those risks, including any specific duration for or terms and conditions on which the risk acceptance is based.

3.2.3.2 After the accredited system is in the operational phase of its lifecycle:

New residual risks identified after C&A activities have been completed must also be accepted by the AO. This can be accomplished by revising the SSP and updating the Risk Assessment Report (RAR). Appending the WCVFs signed by the CIO and the AO (when residual risk exits) will serve this purpose, until these documents undergo formal revision.

The milestone for the corresponding weakness must be included in the POA&M (e.g., "AO Risk Acceptance requires updates to the SSP and RAR to document the AO's risk acceptance decision, terms, duration, and conditions, and any additional required management, operational, or technical security controls to be implemented").

For scenarios that require additional controls to be implemented in order to mitigate the risk to a level acceptable for the AO, those milestones must also be included with details validating their completion.

3.3 Determining Corrective Action Plan Options

There are often multiple methods of remediating a weakness. Various methods should be analyzed to determine the most appropriate corrective action for resolving the weakness and with respect to long-term implications. The system category combined with the security control guidance in *FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems* and the associated *NIST SP 800-53* Revision 3, *Recommended Security Controls for Federal Information Systems and the DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008, are basic factors in the selection of mitigation alternatives. NIST SP 800-53 Revision 3, specifies minimum security controls for systems based on each system's overall security categorization and potential impact ratings (e.g., high, medium, and low) for confidentiality, integrity, and availability. In addition, the cost for each corrective action plan option must be estimated and analyzed to determine short-term and long-term solution capabilities.

The corrective action plan must be well thought out and specifically address the issue it is intended to resolve. A corrective action plan may fully correct a weakness or, alternatively, partially mitigate the weakness to reduce the risk to a level acceptable by the AO. In certain situations, there will be no corrective action planned and risk acceptance will be proposed. (See Section 3.2.2, *Risk-Based Exceptions*)

3.4 Determining Funding Availability

Funding for corrective actions can be obtained through the following means:

- Using current funding marked for security management of the system or program;
- Reallocating existing funds or personnel; or
- Requesting additional funding following the department's and bureau's budget process.

If new funding is required, it is imperative that the department's and bureau's capital planning process is correctly followed to obtain the necessary funds. While the Department requires the reporting of POA&M security costs, which are then reviewed at the department level, the expectation is that the vast majority of remediation costs are to be addressed by each investment's existing base funding or through re-planning of funding from other investment budgets. A medium- or high-risk weakness typically requires immediate attention and cannot wait for a future budget cycle.

Integrating IT security costs with the capital planning process ensures that security is included in the agency's enterprise architecture, supports business operations, and is funded within each information system over its lifecycle.

3.5 Determining an Estimated Completion Date

The estimated date of completion for each corrective action should be based on the outcome of prioritization decisions and in consideration of resource utilization. However, prioritization is not necessarily aligned with completion dates.

Timelines should be realistic and consider all steps and funding needs involved in the level of effort required to correct a weakness. Although several weaknesses may each take 30 days to complete individually, it may not be possible to complete numerous weaknesses during a 30-day period if the same staffing resources are involved. Also, if the corrective action is a long-term solution requiring multi-year funding, then the milestones and completion date should reflect these factors.

3.6 Documenting the Corrective Action Plan in the POA&M

OMB established the foundational structure of the POA&M to provide consistency in the collection and presentation of information. The POA&M module in CSAM was created based upon OMB's POA&M structure. (See Section 4, *Creating and Managing POA&Ms*.)

3.7 Monitoring and Reporting POA&M Activity

The POA&M should be maintained regularly by the System Owner or designee by amending them with newly identified information and updating the status in the comment field of already documented weaknesses as they go through the mitigation process. In addition, corrective actions must be monitored for progress delays, effectiveness, and changes in risk level. Although quarterly POA&Ms provide OMB with a 'snapshot in time' of ongoing activity directed toward improving the overall security posture of DOI's IT environment, ongoing progress monitoring of planned activities is a best practice for any project plan.

3.8 POA&M Weakness Completion Process

FISMA guidance states that the "Completed" status for a weakness should be used only when a weakness has been fully resolved and the corrective action has been tested. Remediation actions must be specific to the weakness identified and ensure slight to no risk of recurrence of the same weakness. Should the weakness recur, there should be compensating controls in place to detect the weakness.

To 'close' a POA&M weakness and consider remediation activity complete, the POA&M must be properly completed and populated in CSAM in accordance with the guidance in this document. The WCVF in Appendix D must be completed and uploaded into CSAM as an artifact as well as evidentiary artifacts that support closure of the POA&M weakness. The WCVF documents all activities and justifications, which must be approved in writing with all required signatures, for closure of all reported weaknesses. This includes corrective action that results in complete remediation or partial remediation with residual risk, or when no corrective

action is taken, which also results in residual risk. In the case of residual risk, the WCVF documents the AO's decision to accept the residual risk.

The WCVF is applicable to weaknesses identified in both the system and program POA&Ms. Copies of these forms become part of the quarterly POA&M package submission and must also be maintained as part of the C&A package documentation for each system to update the SSP and the Risk Assessment Report.

The WCVF is not required for systems that have been officially decommissioned. The decommissioning memorandum must be uploaded into CSAM prior to closing the POA&M weakness.

The following sections outline the process to complete the WCVF required to move a POA&M weakness to a 'completed' status.

3.8.1 Corrective Action Completion

The System Owner (or designee) must review the evidentiary documentation of the completed weakness remediation. Any corrective action must have followed a structured process of implementation, testing, and documentation. Some examples of sources of information that *demonstrate* resolution of a security weakness include, but are not limited to: change control logs (signed/dated/verified or reviewed); test report results related to system changes; contingency/continuity of operations test reports; contingency plan testing with documented results of table top exercises; hard-copy user access control/review lists (signed/dated); contingency plans/tests (signed/dated).

The System Owner must also evaluate the risk-impact level of any residual risk. In cases where no corrective action is taken, the System Owner must document the rationale and justification for risk acceptance. Similarly, in cases where the corrective action for a high-level risk results in only partial mitigation and the residual risk level is subsequently reported as medium or low, the System Owner must document the rationale and justification as to why he or she now considers the reported weakness risk level to be less than high.

The System Owner then completes and signs off on the WCVF, Part I attesting to the implementation of the corrective action and update the milestones in CSAM accordingly.

3.8.2 Independent Verification of Corrective Action Completion

Corrective actions must be independently verified and tested to ensure that remediation efforts affect the intended results and adequately address the security weakness. This process also verifies that remediating controls are in place and that any other known remaining residual risks have been identified.

The independent reviewer should not be an individual who plays an active role in managing the system under review as this is considered a conflict of interest and may hinder a truly independent evaluation of documentation or technical solutions. The Regional Information Security Officer (RISO) or BCISO are individuals who can fill the role of independent reviewer, but the role is not limited to these personnel. It is up to the bureau or office to designate

appropriate independent reviewers. However, POA&Ms created as a result of an OIG evaluation must remain open until the Cyber Security Division (CSD) POA&M and Audit Liaison Service Area has the opportunity to re-evaluate them and confirms they are resolved to their satisfaction (See Appendix F, *OIG Recommendation Audit Reporting Process*).

The independent reviewer will review documents compiled by system teams or perform other testing as necessary to ensure that technical solutions implemented as the corrective action are working as intended and satisfactorily address the identified weakness. The review process may include 'shoulder surfing' or visual inspections of technical solutions, documentation reviews, and inspections and evaluations of technical tests results. The independent reviewer must document the assessment method and his or her findings and sign the WCVF, Part II.

3.8.3 Bureau CIO Review of Corrective Action Completion

Bureau CIOs are responsible for reviewing and approving all completed corrective actions. The CIO has the option of rejecting the 'Completed' status of system security weaknesses. If this occurs, the previously completed or accepted weakness will be returned to the system or project team and the POA&M weakness will be re-created in CSAM with a revised corrective action plan. The re-created (new) POA&M **must** reference the original POA&M ID number in the "POA&M Title" field. Additionally, the original (old) POA&M **must** reference the re-created POA&M ID number in the "POA&M Title" field.

Bureau CIOs will review the WCVF and other evidentiary documentation as needed to evaluate a completed system security weakness and verify that internal controls associated with the POA&M reporting process are working as required. CIOs must sign the WCVF, Part IV, attesting to the fact that corrective actions have been implemented correctly prior to closing the weakness in the POA&M.

3.8.4 AO's Acknowledgement and Acceptance of Risk(s)

The AO is responsible for thoroughly reviewing all residual risk recommended for acceptance by CIOs, System Owners, System Security Managers, or BCISOs. The AO can either approve or reject the recommendation. If the AO chooses to reject the recommendation, then the POA&M weakness must be re-created in CSAM and a revised corrective action plan must be prepared. This is an extension of the AO's role of accepting or rejecting risk in the issuance of an ATO.

In accordance with the *Information Technology Security Policy Handbook*, in considering whether or not to accept the risks indefinitely or for some specified time, the risk acceptance documentation must identify any conditions and constraints under which those risks will be accepted by the cognizant AO (e.g., specified acceptable duration within which the AO will tolerate continued acceptance of the risk, any required mitigating actions and/or compensating controls to be implemented as interim protective measures, etc.) Where the AO is unwilling to accept risks indefinitely, the weakness must be incorporated into the appropriate program- or system-level POA&M. These are the appropriate means, and only formal methods available, that are consistent with FISMA, OMB, and NIST standards and guidelines by which weaknesses are effectively understood, documented, accepted, managed, and tracked. There are no provisions to request any other form of exemption to policies and standards.

To consider the remediation complete, the AO must acknowledge the residual risk of each completed corrective action and indicate his or her acceptance by signing the WCVF, Part V. If a corrective action fully mitigates all risk, then it is not necessary for the AO to review the WCVF.

In order for the AO to fulfill this responsibility, the CIO, System Owner, BCISO or AO's designated representative should provide quarterly briefings to the AO to facilitate the risk acceptance process.

All high-risk weaknesses must be corrected if possible or otherwise mitigated to at least a medium level of risk. The AO can only consider acceptance of medium or low risks. When economically feasible, every effort must be made to correct or further mitigate all risks to a level commensurate with the potential impact to systems and associated data.

The AO is the **only** official authorized to accept security risks for the systems under his or her purview and they must document their acceptance of those risks.

3.8.5 Documentation Updates

When identifying weaknesses, completing corrective actions, or accepting risk, in addition to the POA&M, other documentation must be regularly updated.

- **System Security Plan** – The SSP must be updated when controls are changed or added to a system as part of a corrective action plan. Also, the formal acceptance of risk in a required control category should be documented in the SSP. Until the SSP is formally revised, however, appending the WCVF and supporting documentation to the SSP will satisfy this requirement.
- **Risk Assessment Report** – The Risk Assessment Report must also be updated if there is long-term residual or accepted risk. Appending the WCVF and supporting documentation to the Risk Assessment Report will satisfy this requirement.

3.8.6 Weakness Completion Follow-Up

Periodically, or at least quarterly, all residual and accepted risks associated with a weaknesses should be reviewed to determine whether changes in architecture, security controls, technology, exposure (e.g., to the Internet or other internal/external system interconnections), information sensitivity, or business practices have altered security risks for the system. If overall risks (risks at the aggregate level) have increased, the responsible officials should take appropriate measures, including adding a new system weakness to the POA&M. All risk related actions and periodic reviews must be updated in the POA&M milestones accordingly.

3.9 POA&M Quarterly Certification Transmittal

The Certification Transmittal requires that bureau CIOs review all aspects of their organizations' program and system POA&Ms for the current quarterly submission. The objective is to ensure that the POA&Ms are completed in accordance with the standards described within this *POA&M Process Standard* as per DOI OCIO Directive 2006-007.

The Certification Transmittal also requires that each AO within the bureau or office review all aspects of the system POA&Ms for which he or she is responsible. The intent is to ensure that the AOs have been briefed on and understand the current security status of the systems for which they are responsible. This covers the risks relating to the current set of unmitigated weaknesses, not just the risks that they have formally accepted as part of the C&A process and the POA&M weakness completion process. Because there may be more than one AO within a bureau or office, the Certification Transmittal is divided into two sections. A Certification Transmittal from the CIO and a separate Certification Transmittal from each AO.

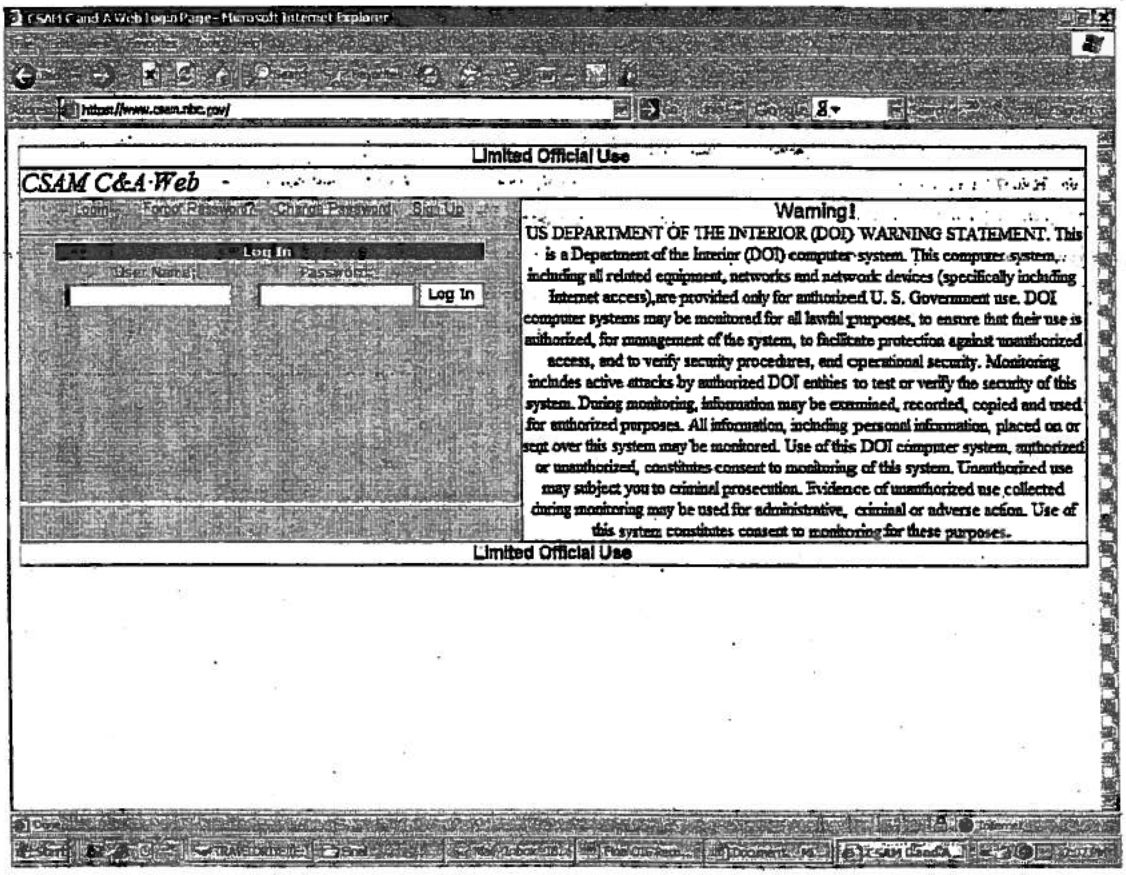
CIO Certification Transmittal – The bureau CIO will review the quarterly POA&M packages submitted by each of the bureaus and provide a signed Certification Transmittal covering all systems, certifying the POA&Ms compliance and acceptability. The quarterly Certification Transmittal must list all of the systems for that bureau or office, their operational status, and their C&A status. (See Appendix E, *POA&M Certification Transmittal*) The AO Transmittals are appended to the CIO Certification Transmittal.

AO Certification Transmittal - AOs will review the POA&Ms for systems they are responsible for and provide a signed Certification Transmittal attesting to their acceptance of the security posture of the system. (See Appendix E, *POA&M Certification Transmittal.*)

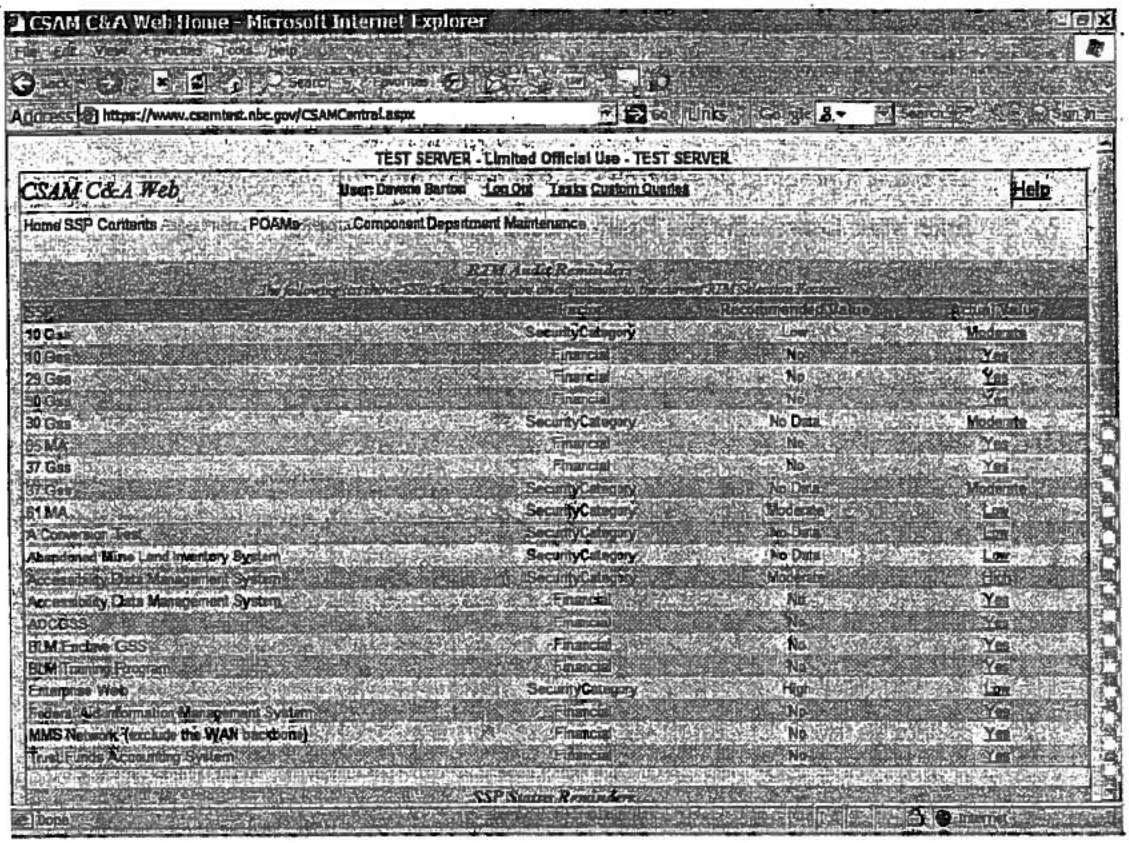
4. Creating and Managing POA&Ms

This section will explain how to create and manage program and system POA&Ms in CSAM. Please refer to Appendix F, *Office of Inspector General Recommendation Status Reporting Process*, for guidance on POA&M weaknesses that are created as a result of an OIG evaluation.

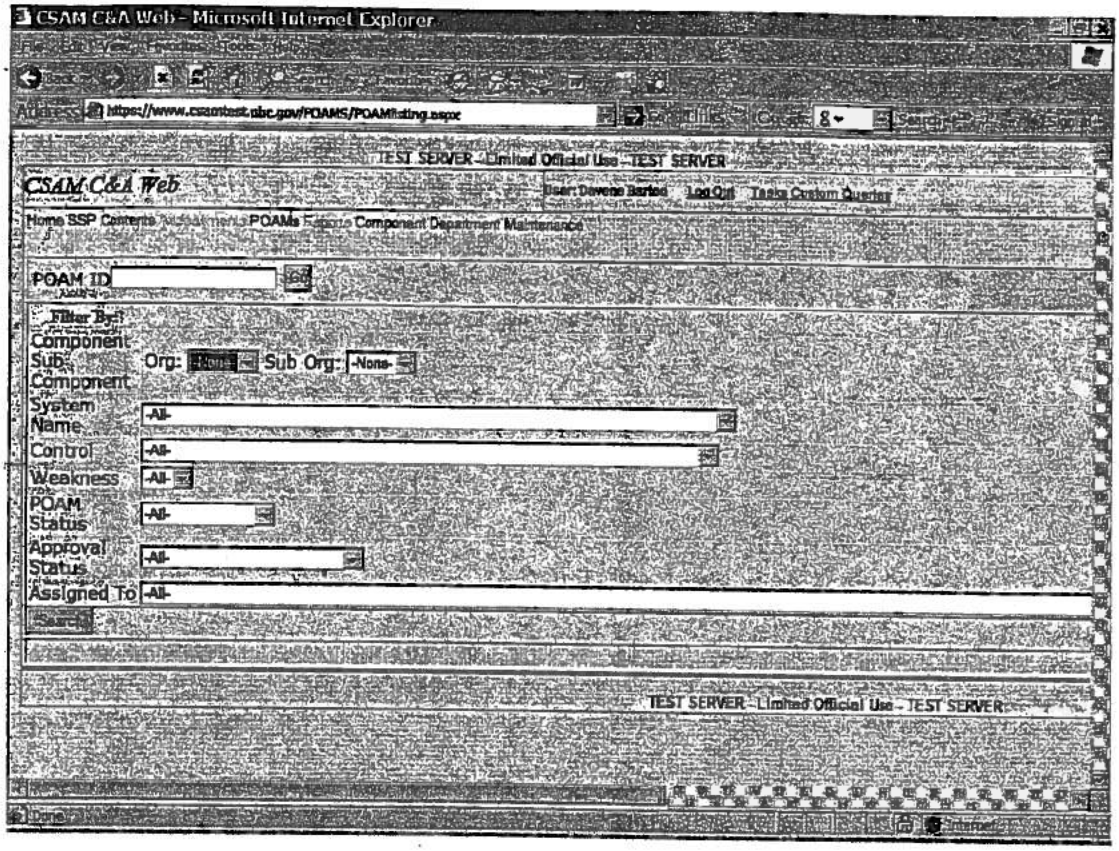
1. To create a program or system POA&M go to: https://www.csam.nbc.gov.
2. Enter your User Name and Password and then select **Log in.**



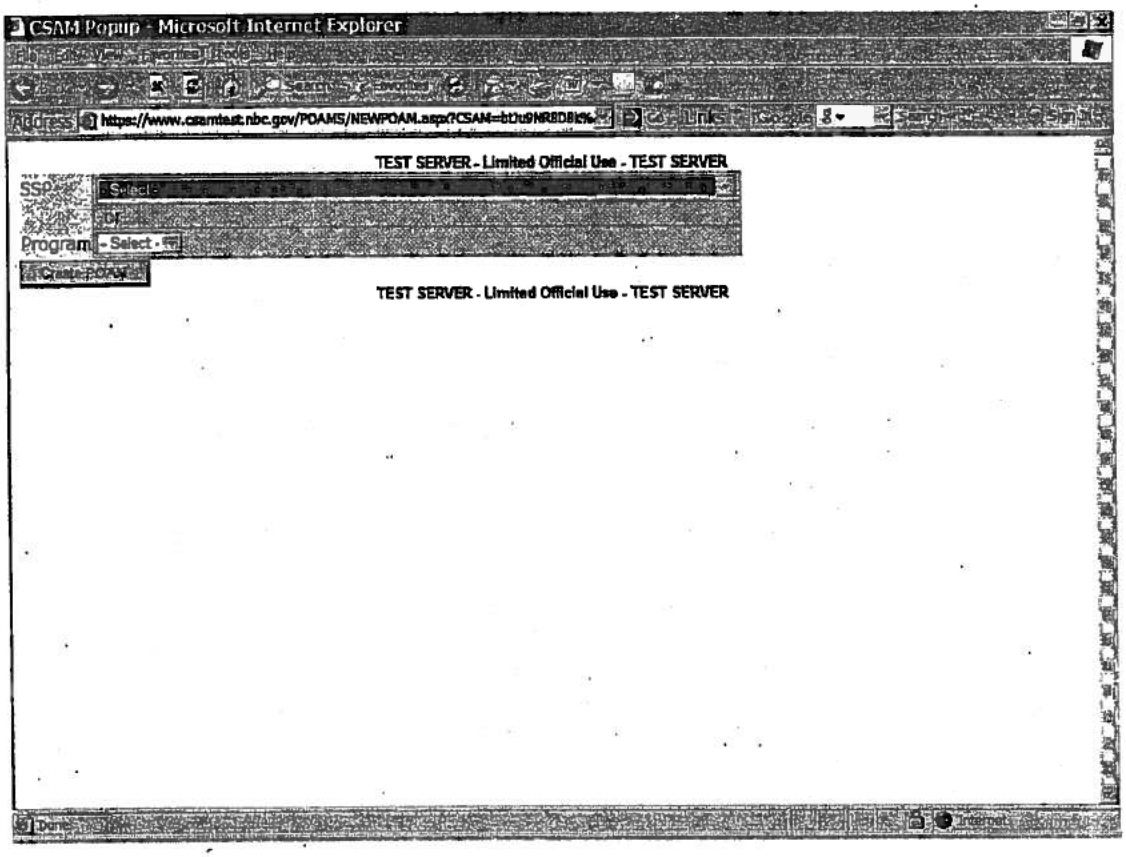
3. Select the **POA&Ms** link.



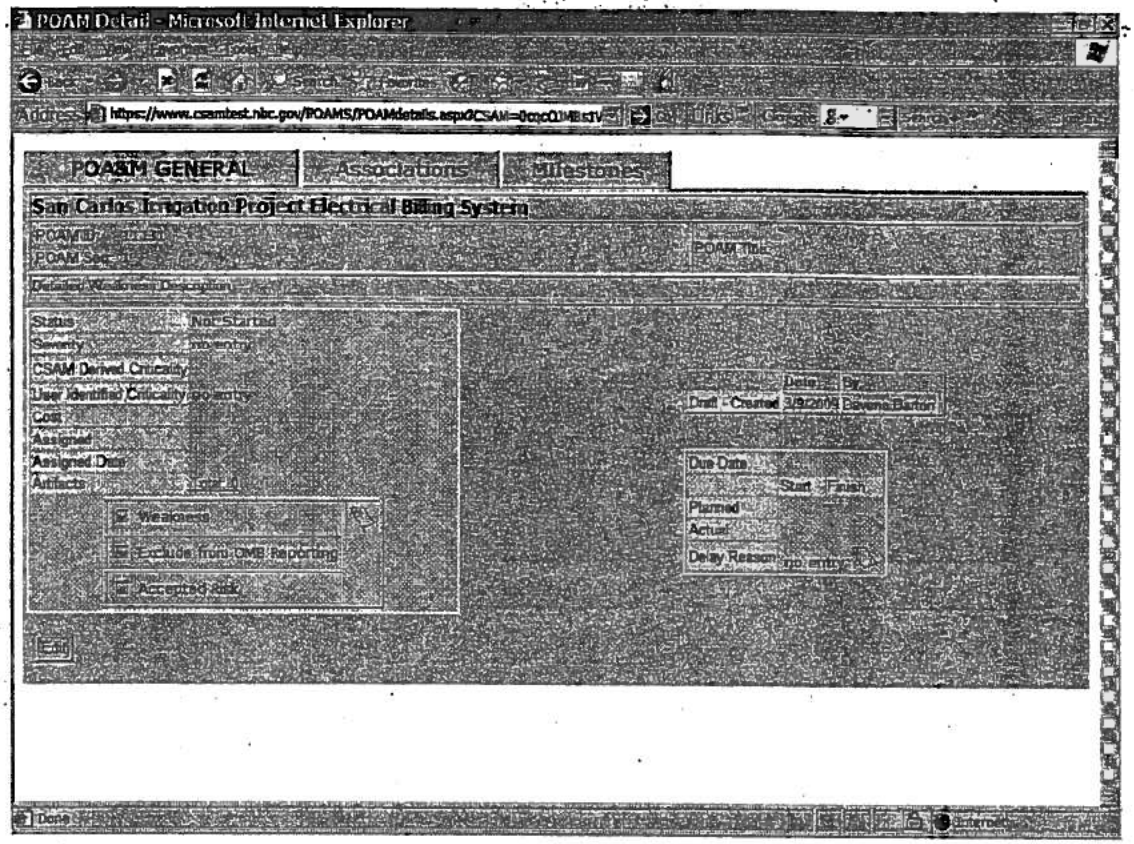
4. Select your bureau/office (**Org**) name, select **System Name** and then click the **Add POA&M** button located on the far right side of the screen.



5. Select the **Program** or **SSP** (system) name from the pick list and then select **Create POA&M.** (Note: Users will only have access to the systems/program specific to their bureau or office).

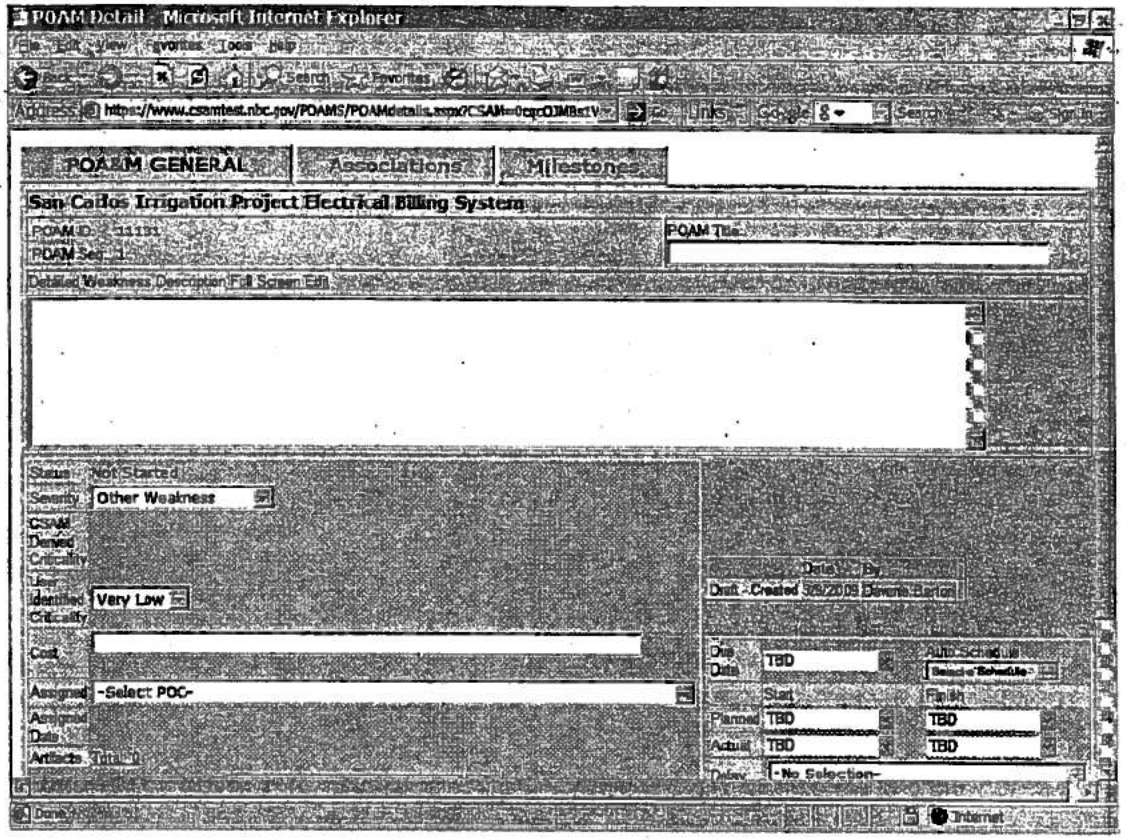


6. Select **Edit**.



The **POA&M ID** is a CSAM generated unique number for each POA&M. This number is unique amongst all system, site and program POA&Ms.

The **POA&M Seq.** is a CSAM generated unique number for each POA&M. This number is unique only within the system, site or program it belongs to. This number is sequentially assigned.



7. Enter **POA&M Title** - a brief description of the weakness.

8. Enter **Severity** by clicking the drop- down menu and choosing the applicable option. The options are as follows:

   a. **Other Weakness**: The PAO&M is not related to a specific control and was determined in a fashion other than the other options available for selection.

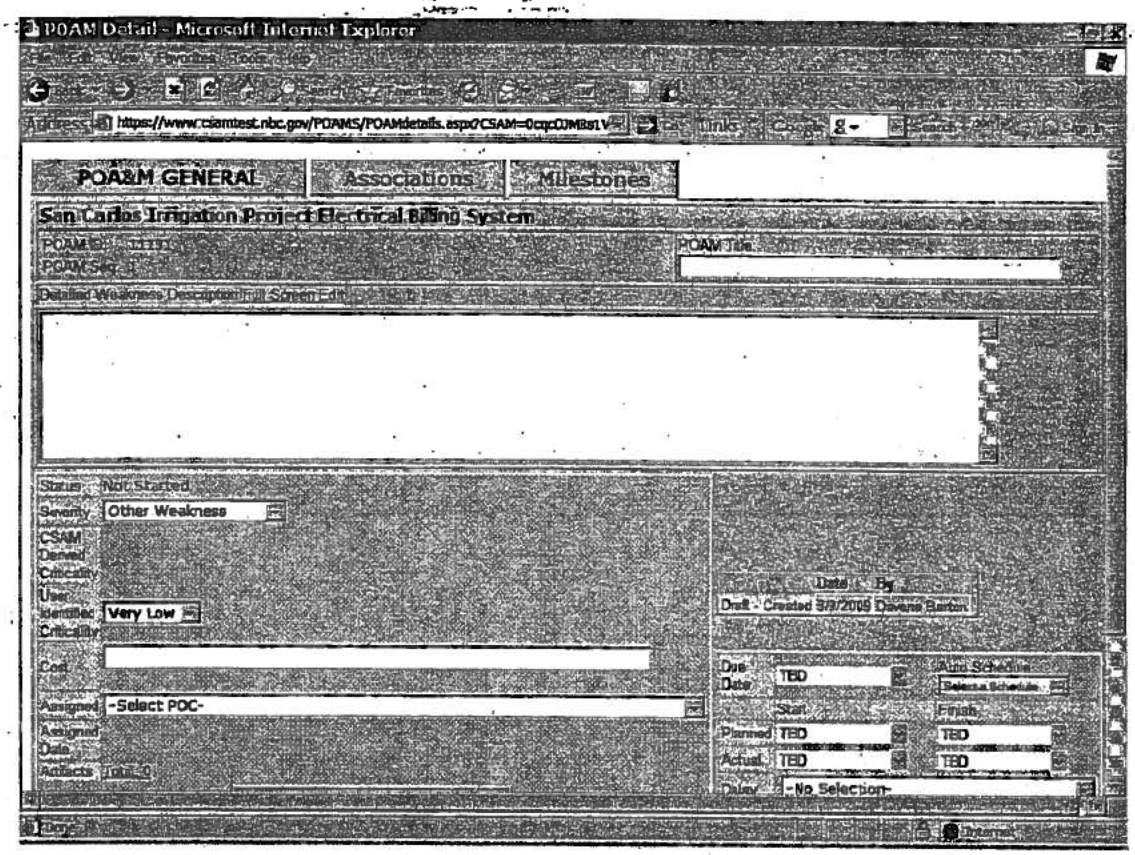
   b. **Control Deficiency**: The POA&M is related to a control that is not implemented for a given system/program.

   c. **Significant Deficiency**: The POA&M is not related to a specific control that is not implemented, rather the POA&M is related to another significant finding.

   d. **Reportable Condition** (Deprecated): Deprecated means that this option should no longer be used by or selected by the user.

   e. **Material Weakness**: The POA&M is not related directly to a control that is not implemented, rather the POA&M was found as a material weakness by an external examination (audit or some other means).

9. Enter **Detailed Weakness Description**. Enter the detailed weakness description in the text box.



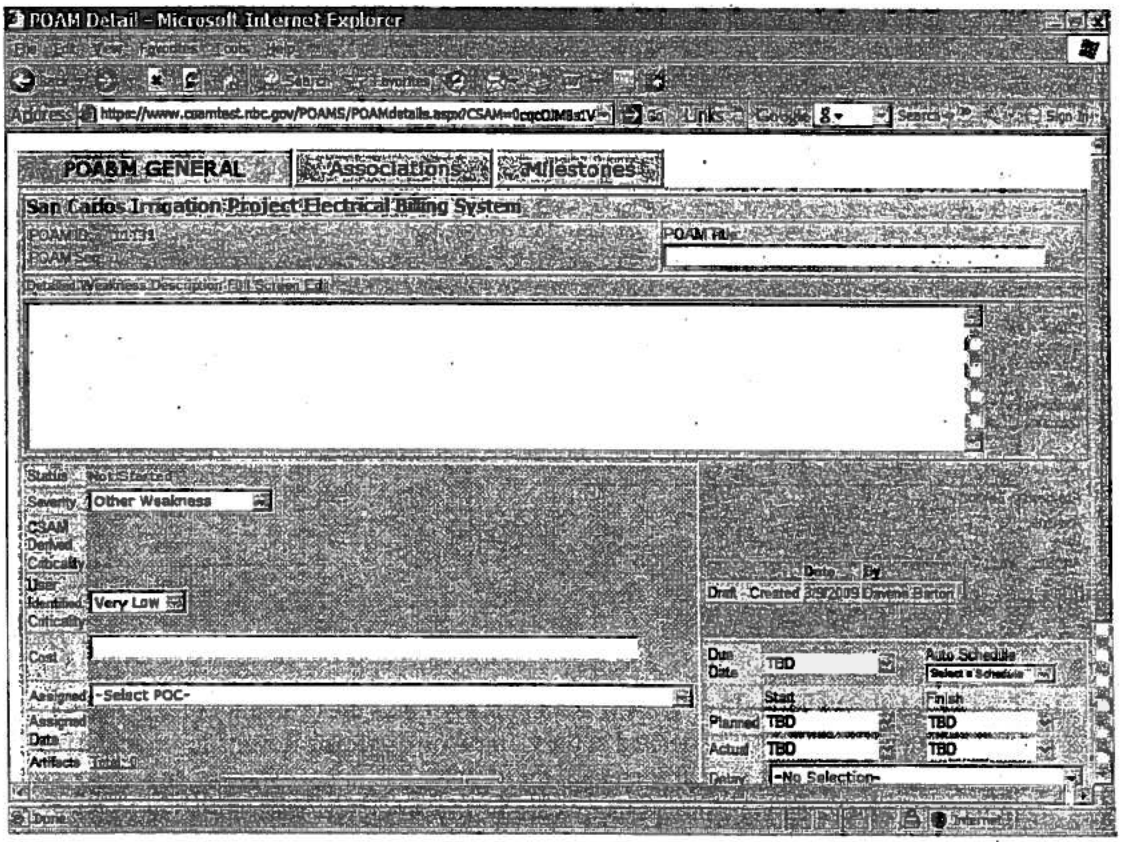
10. **CSAM Derived Criticality**. CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level and is unaware of the operating environment of the system (i.e., is not aware of any mitigating/compensating controls that would justify any lower risk rating – e.g., a vulnerable port/service might have an initial risk rating of high but when taking into consideration an external firewall that prevents any other system from accessing the vulnerable port/service the user identified risk level might be adjusted to medium or low).

    The **CSAM Derived Criticality** value is dynamically updated as the associated control implementation status changes. In the event the vulnerability is not associated at the control or expected result level, the user identified criticality level must be populated. An example of this may be Program related vulnerabilities.

11. Select the **User Identified Criticality** of the POA&M from the pick list. Using data from a user defined risk assessment process, enter appropriate the criticality level. (Note: The User Identified Criticality level is the "official criticality level" to the extent that it is selected/identified as instructed by this POA&M Process Standard. If it is not adjusted

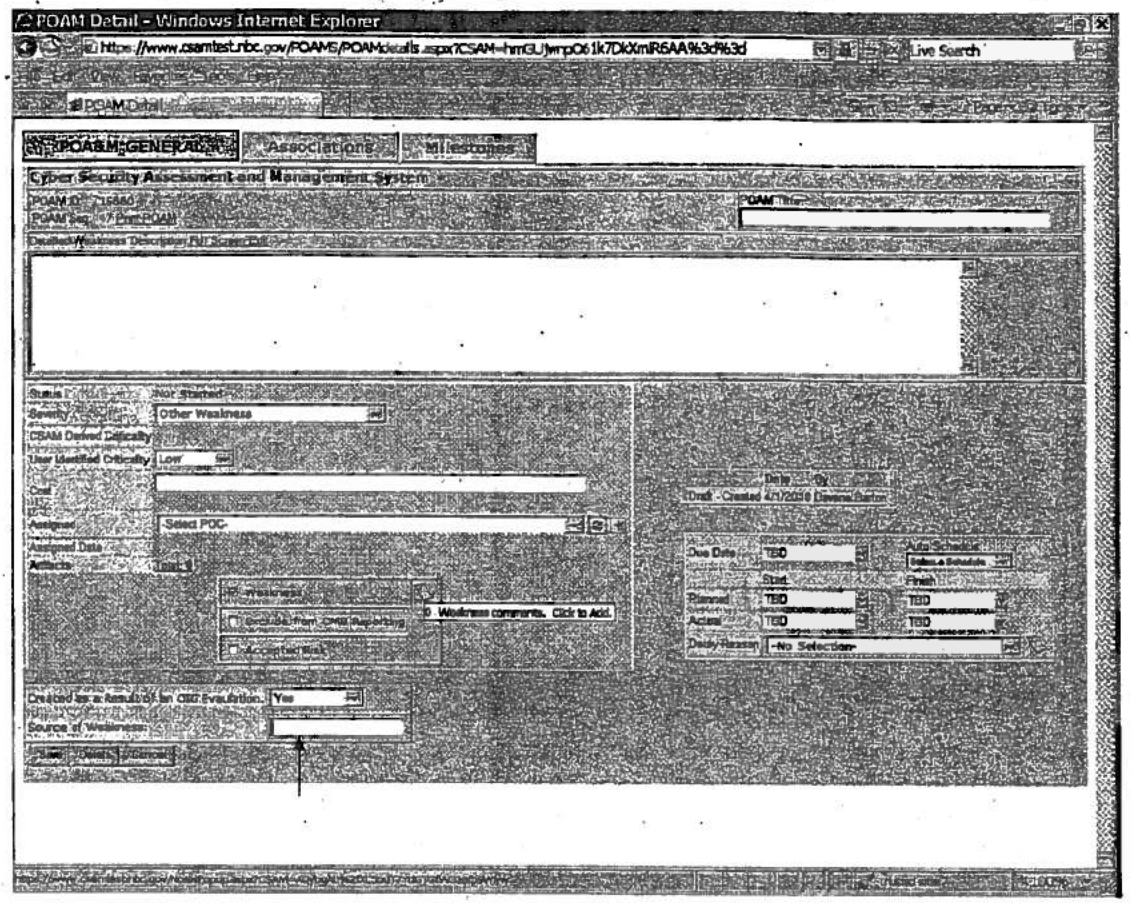
by the user then the "official criticality level" would default to the "CSAM Derived Criticality".

12. Enter the **Cost** information. POA&M cost can be captured and associated with the POA&M, providing visibility on several other CSAM screens. This capability enables IT Security Specialists and management to make credible, risk-based decisions with regard to the operation and use of information systems.

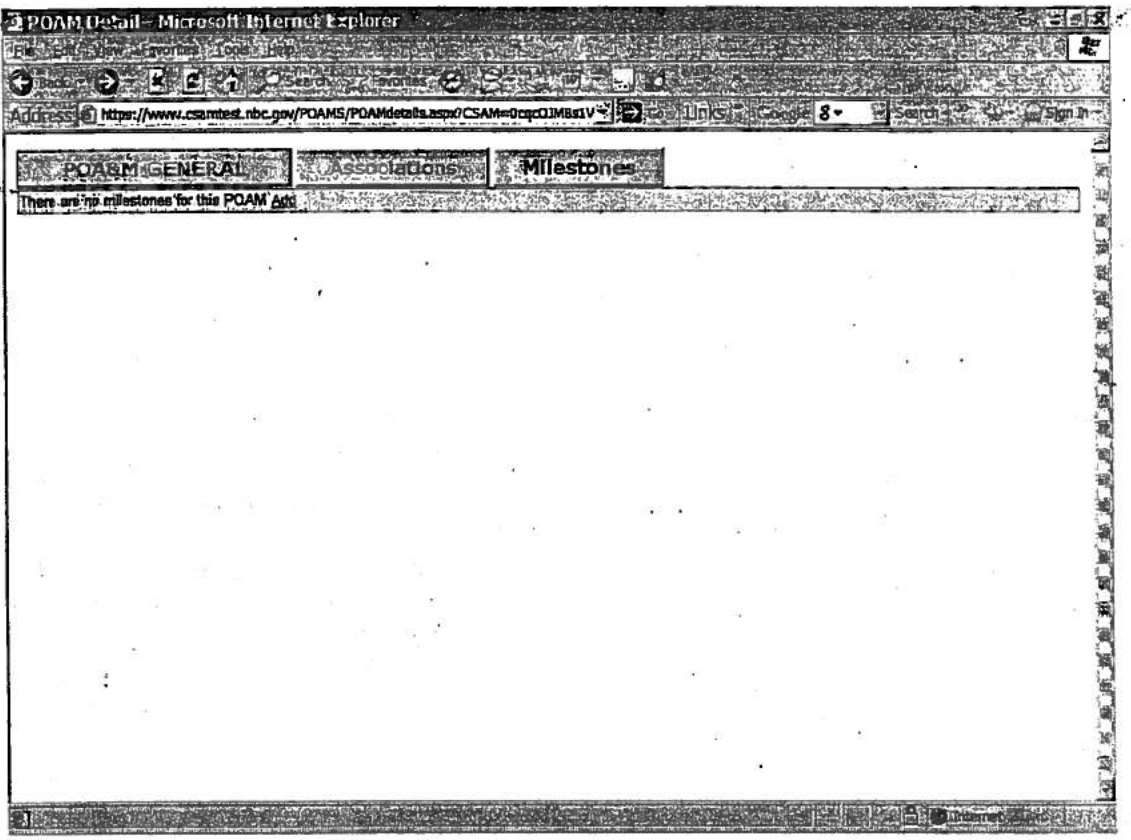


13. Enter **Assigned POC**. This assignment is made from a drop down table of POCs for which CSAM contains contact information online.
14. Enter the **Due Date** also known as the Schedule Completion Date (SCD). This date is the key date that will be locked-down as the baseline, once the POA&M is approved. While in Draft POA&M status, this value can be changed. The user has the option to enter dates directly into individual fields or use the auto-scheduler to set the **Due Date, Planned Start** and **Planned Finish** dates, however, the user must enter the **Actual Start** and **Actual Finish** dates manually.
15. Select **Yes or No** from the **Created as a Result of an OIG Evaluation** pick list, enter the **Source of Weakness. When entering the source of weakness information bureaus/offices must include the title of the report, the report**

number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.
Click Save.



16. Select the **Milestones** tab and then select **Add.**
17. Enter milestones in the order they should be executed.



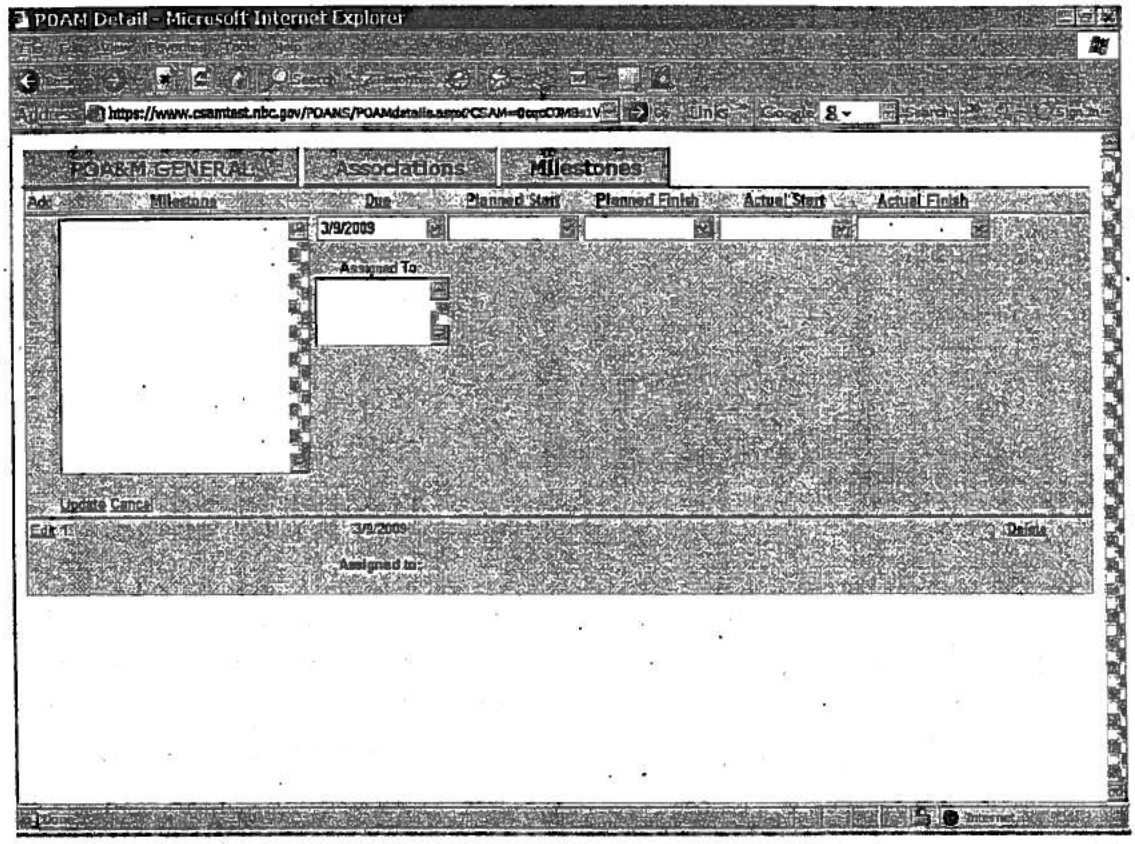
Note: The key milestones associated with each corrective action should be identified on each POA&M. Each weakness must have one or more associated milestones. Milestones should define the major steps that will be performed to complete the corrective action. If there is more than one milestone, enter the milestone in the order they should be executed. For example, one set of milestones for a weakness such as, "Identification and authentication are not adequate for the level of security controls required for this system" might be:

1) Evaluate methods for strengthening identification and authentication.
2) Recommend solution and obtain approval.
3) Develop procedures to standardize accepted identification and authentication process.
4) Design identification and authentication solution.
5) Build identification and authentication solution.
6) Test identification and authentication solution.
7) Deploy identification and authentication solution and implement supporting process.

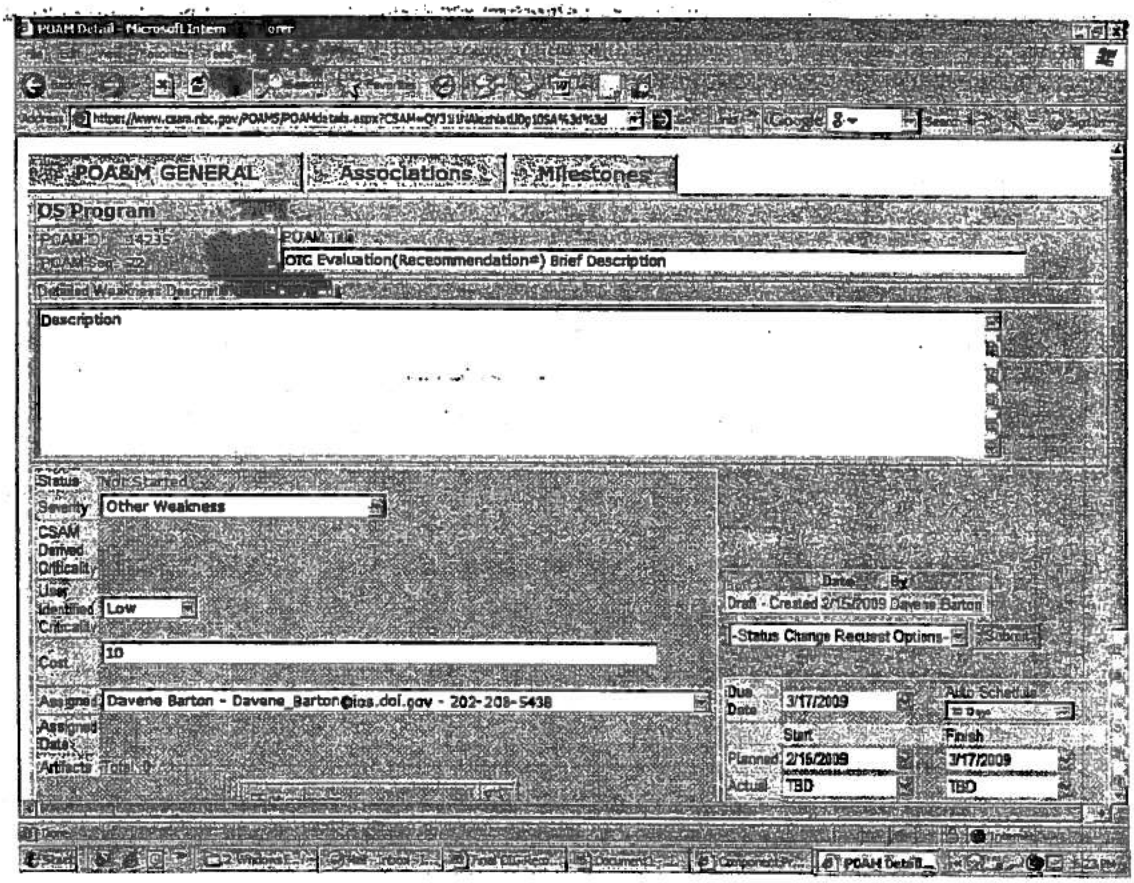
Milestones might also include more specific aspects related to the technical solution (e.g. implement two-factor authentication), and management and operational controls related to the steps for implementing supporting business practices and procedures where additional security control requirements are known or anticipated.

The description of each milestone must be detailed enough so that an independent reviewer will understand the planned corrective action and determine whether the corrective action is adequate and appropriate and will result in the weakness being corrected or its associated risk mitigated to a level acceptable to the AO. The last milestone entry must clearly identify the action taken to mitigate the weakness. Sensitive information can be included as needed for the description since the entire POA&M is a sensitive but unclassified document.

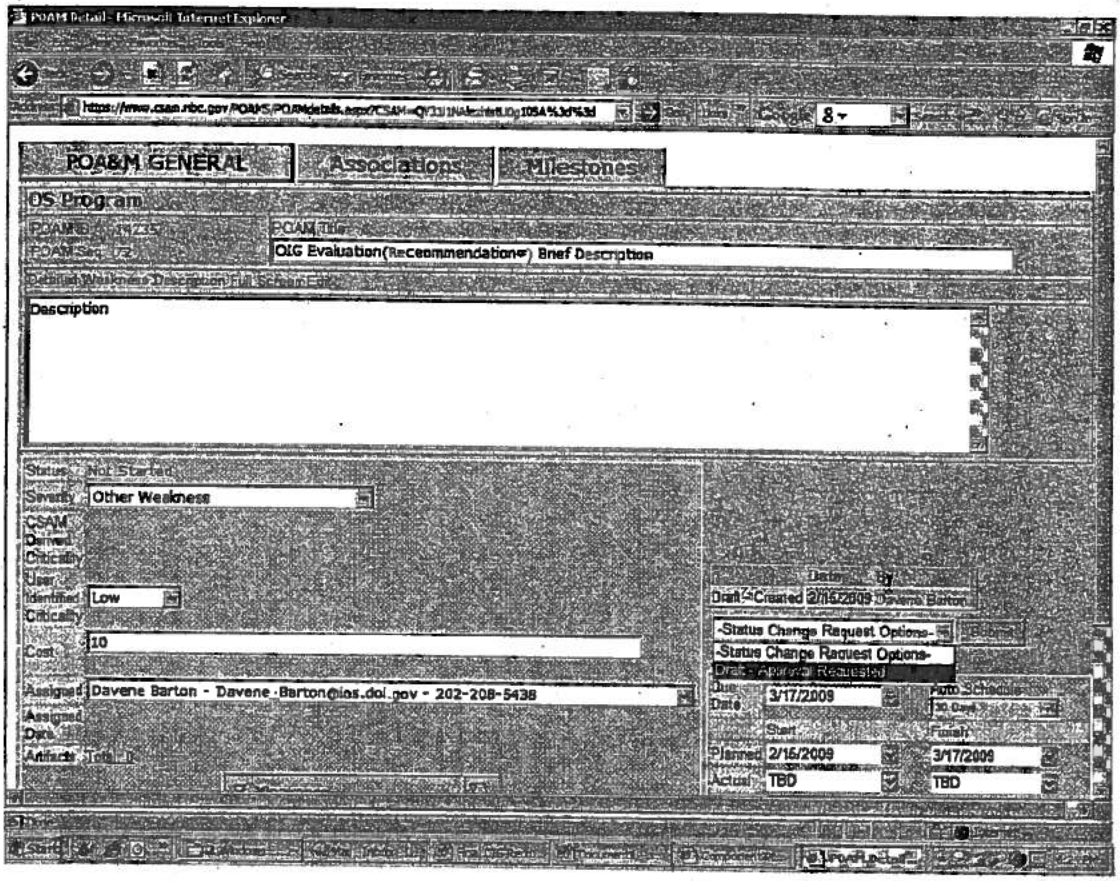
18. Select **Update** to save the entry.



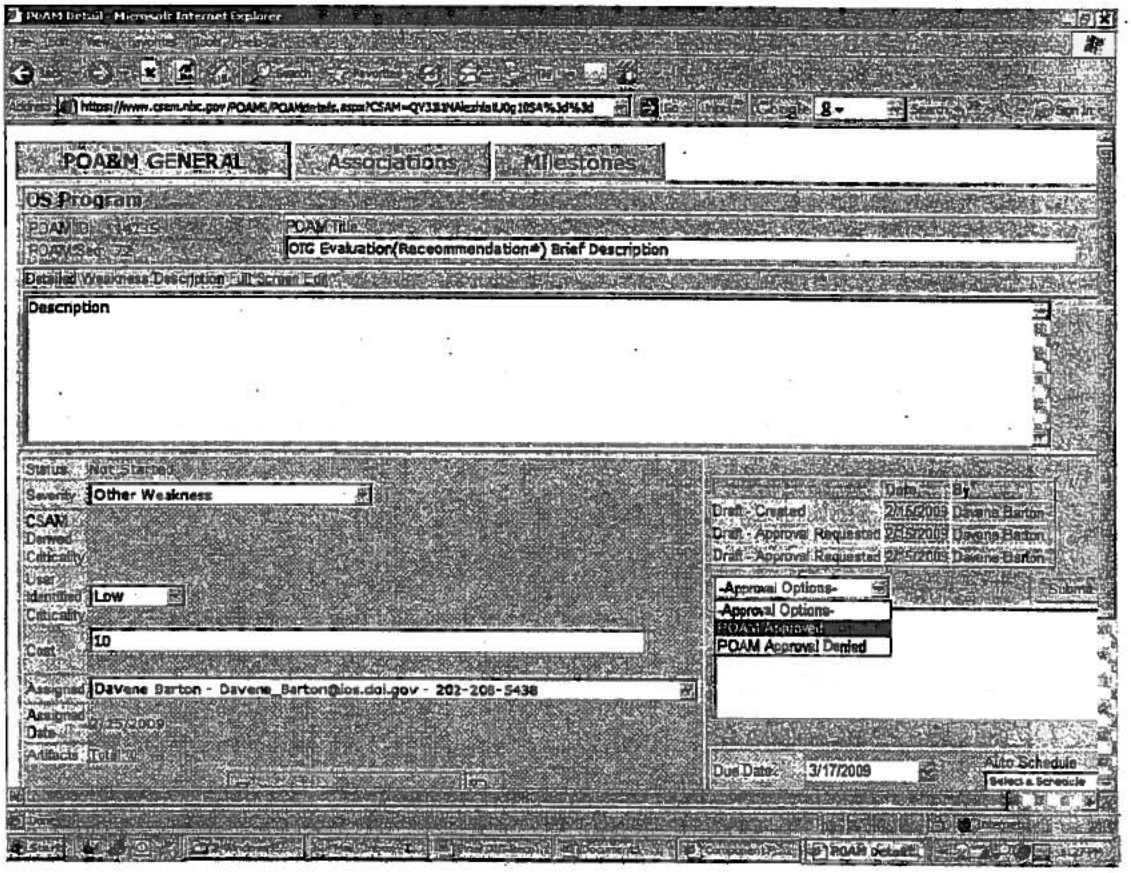
19. Select the **POA&M General** tab and then select **Edit**.



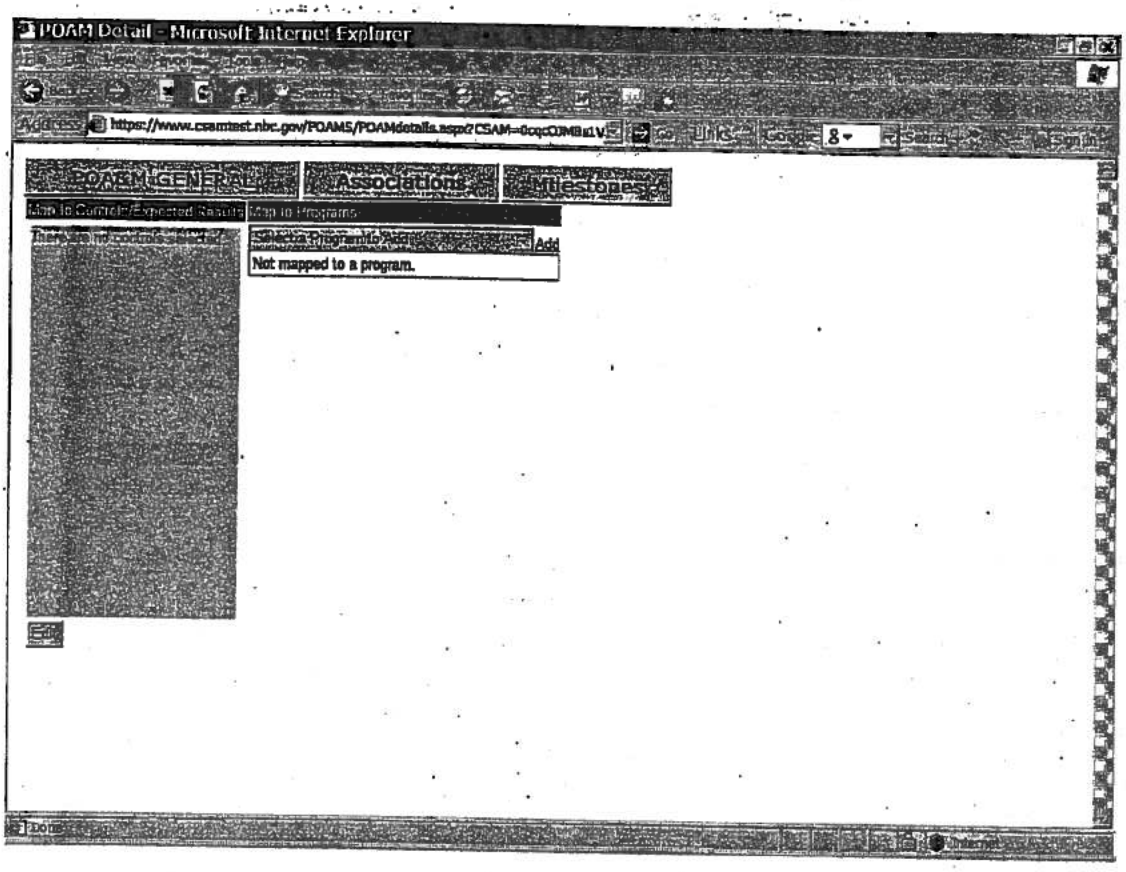
20. Select **Draft – Approval Requested** from the **Status Change Request Options** pick list and then click **Submit**.



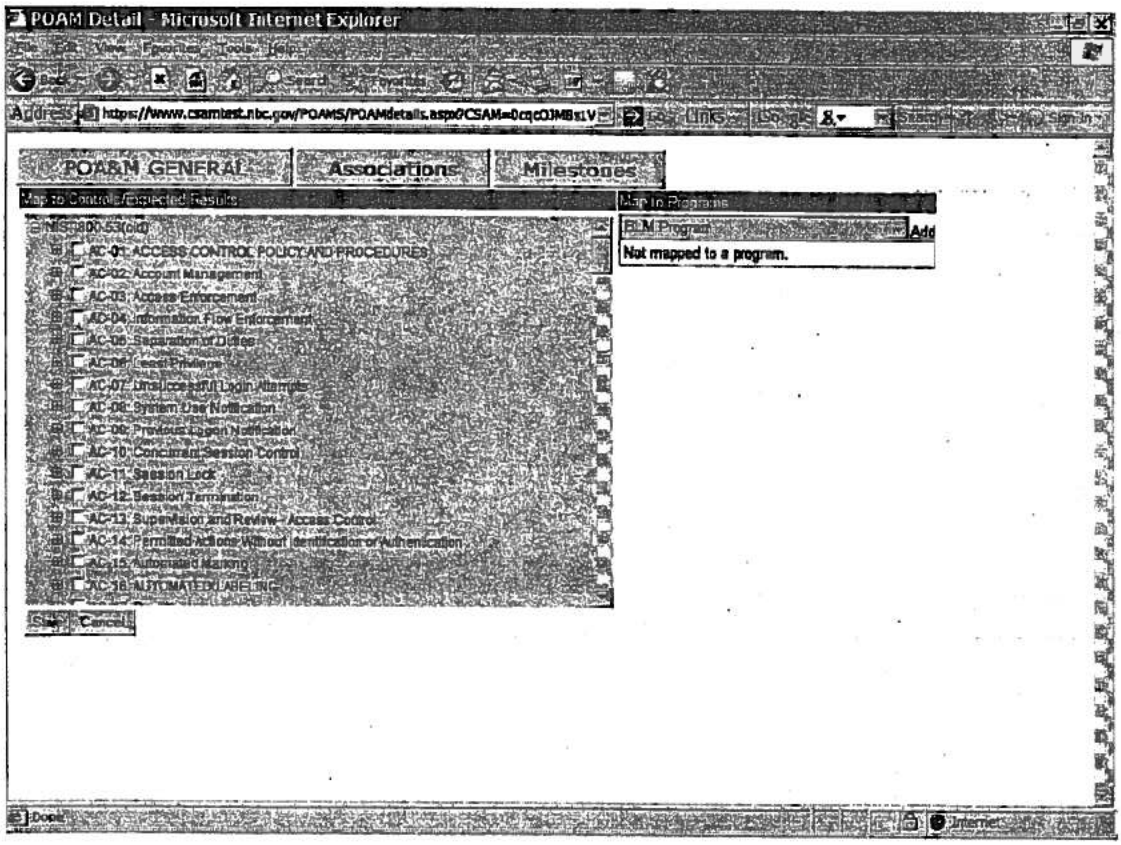
21. To approve entry of the POA&M, select **Edit, POA&M Approved** from the **Status Change Request Options**, provide comments and then click **Submit**.



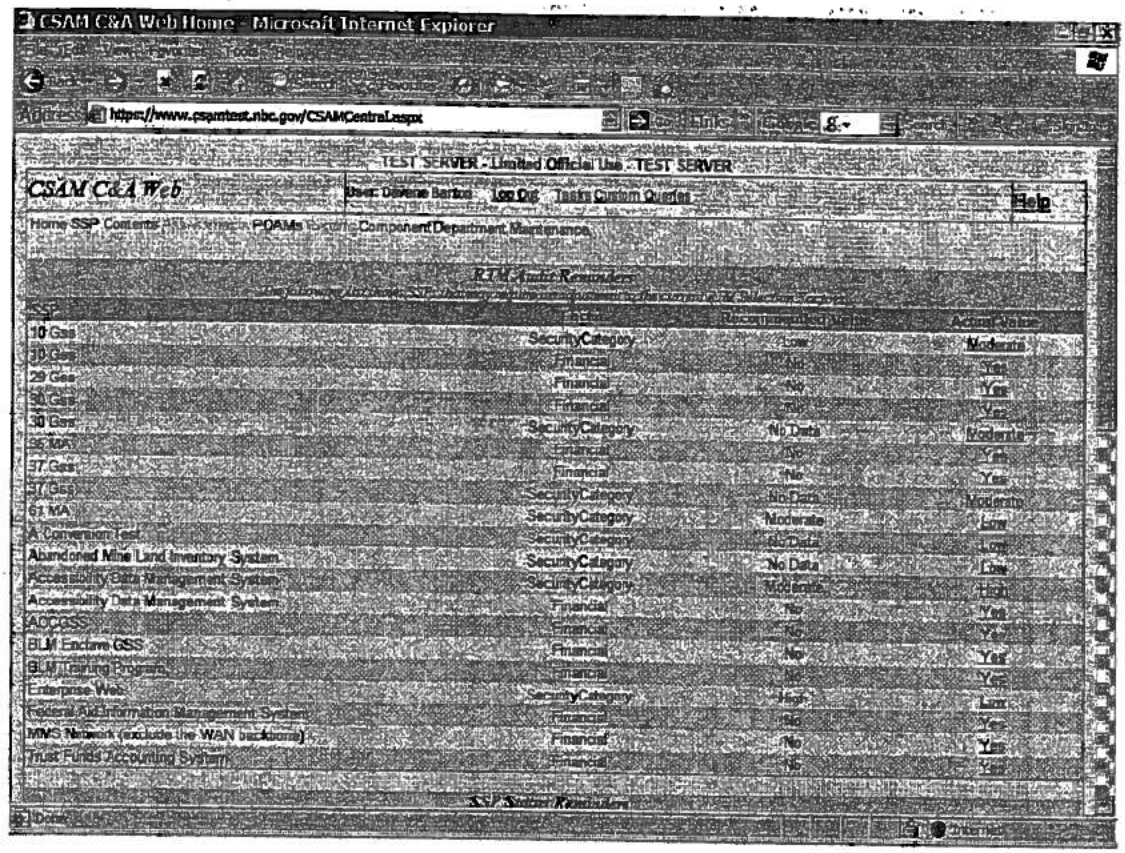
22. Select the **Associations** tab to tag multiple controls and expected results.



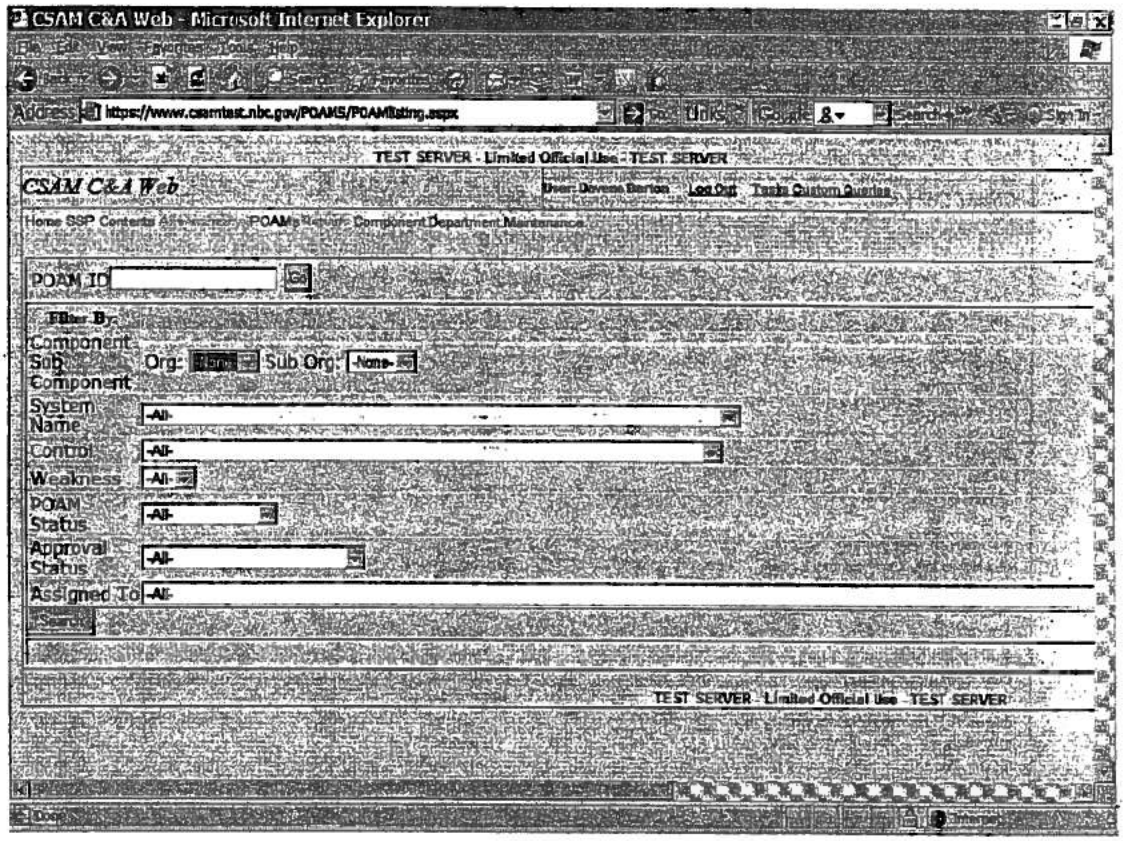
23. Select **Edit**.
24. Select applicable controls.
25. Select a Program to add (if applicable) and then select **Add**.
26. Select Save.
27. Select the **POA&M General** Tab and exit the application. This completes the POA&M creation work flow process.



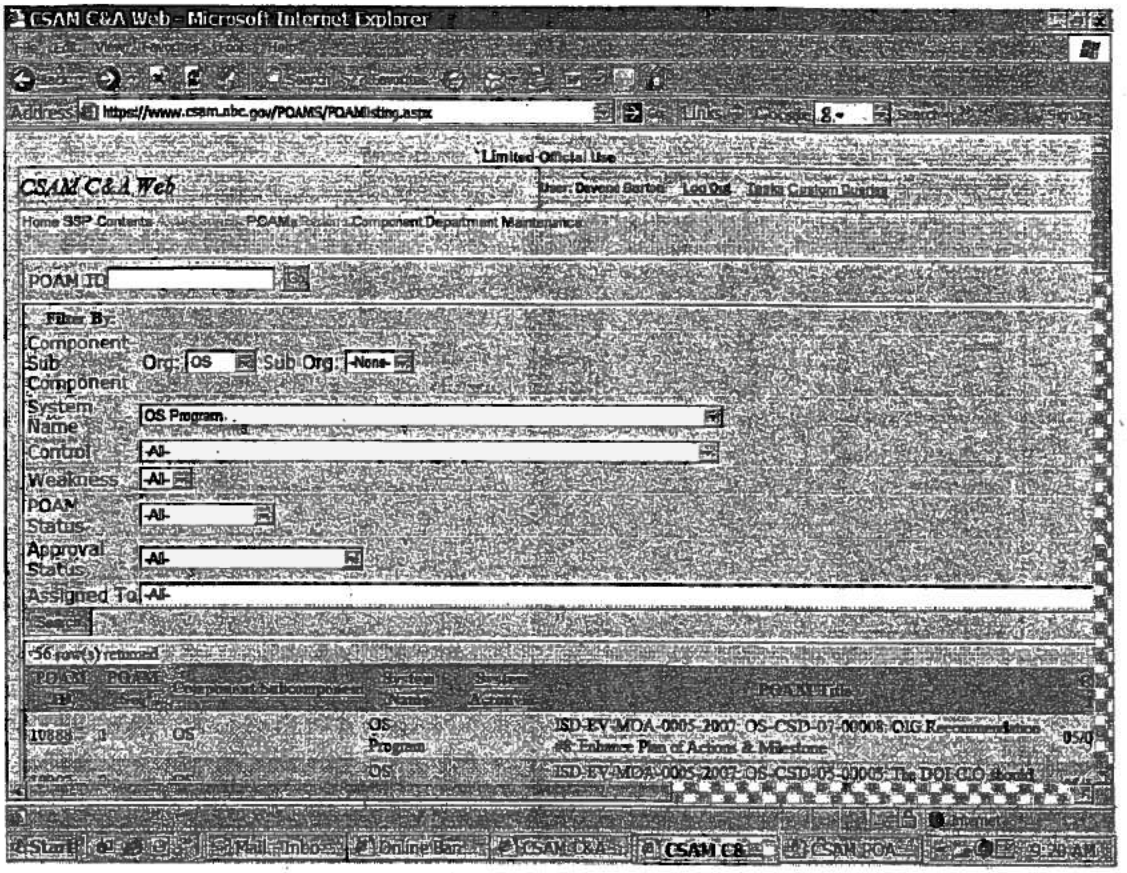
28. To close a POA&M weakness, select the **POA&Ms** link.



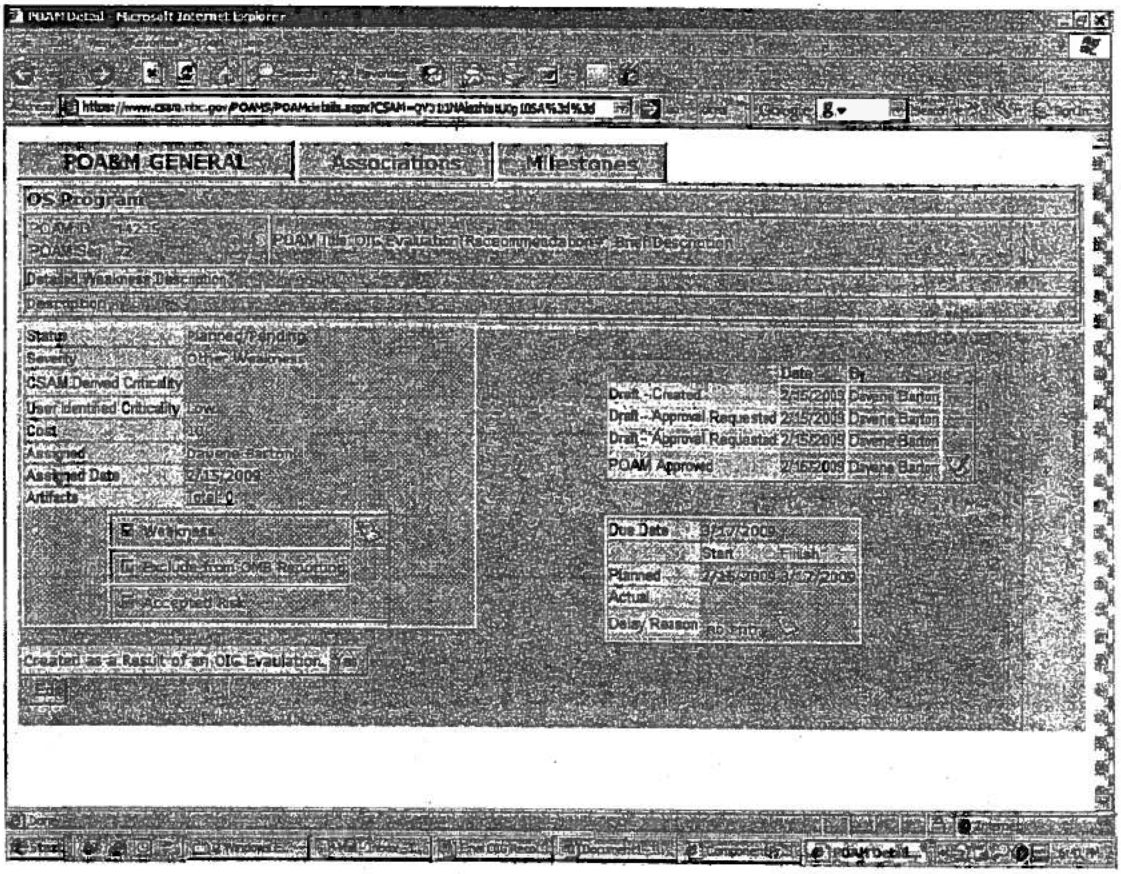
29. Select your bureau/office(Org) name, select **System Name** and then select **Search**.



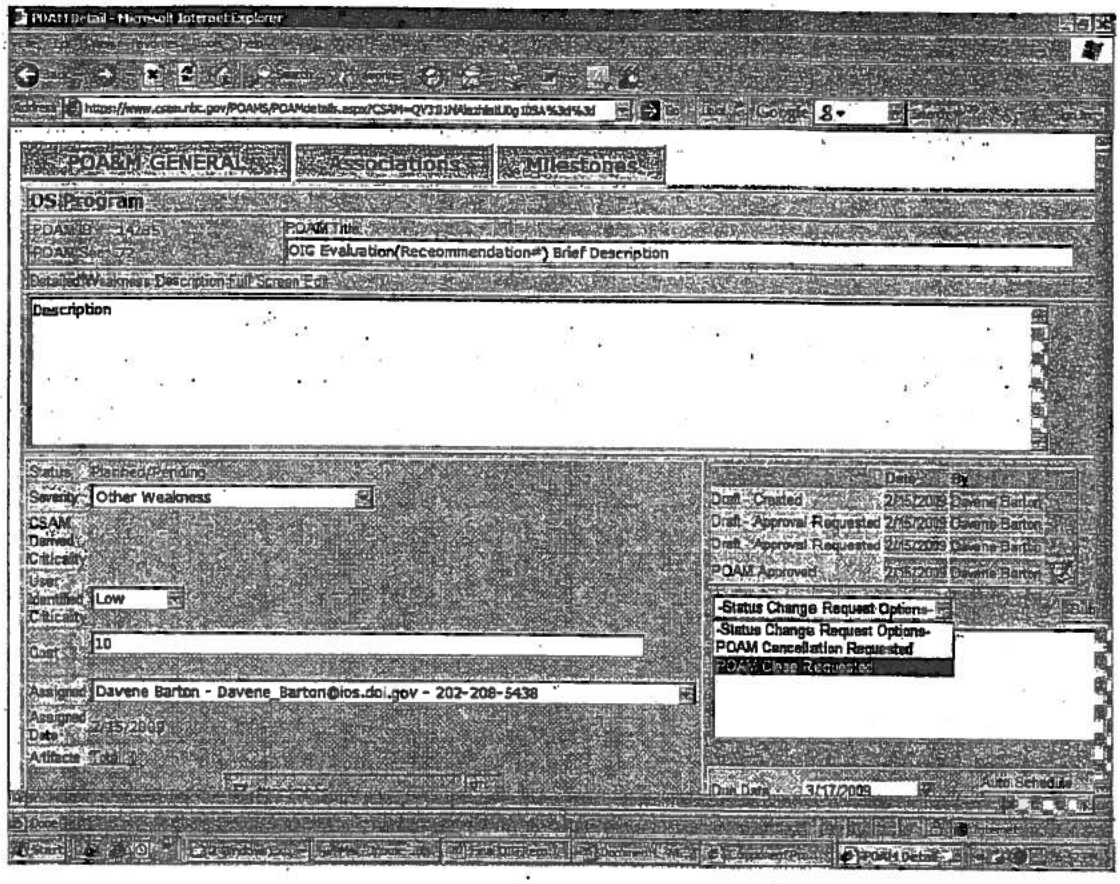
30. Enter the **POA&M ID** that you would like to close and select **Go.**



31. Select **Edit**.

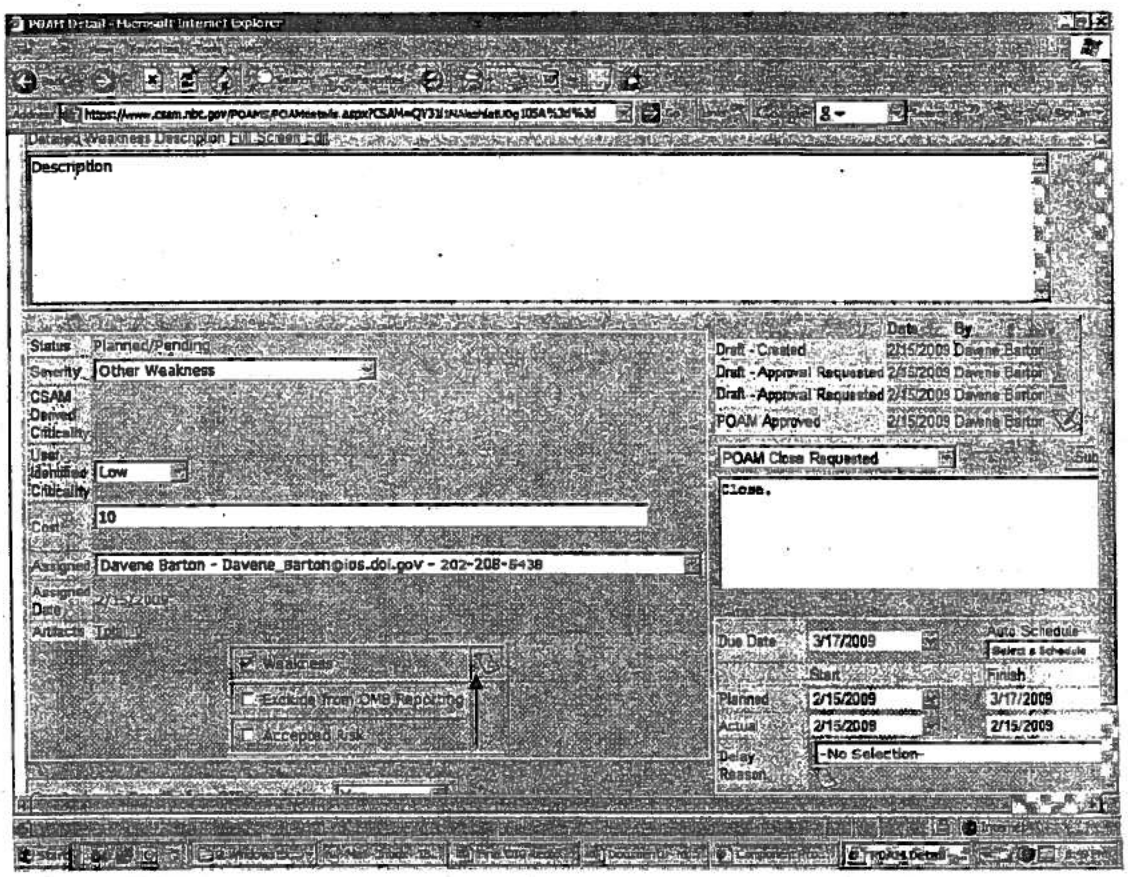


32. Select **POA&M Close Requested**, from the **Status Change Request Options**, provide comments and then click **Submit**.

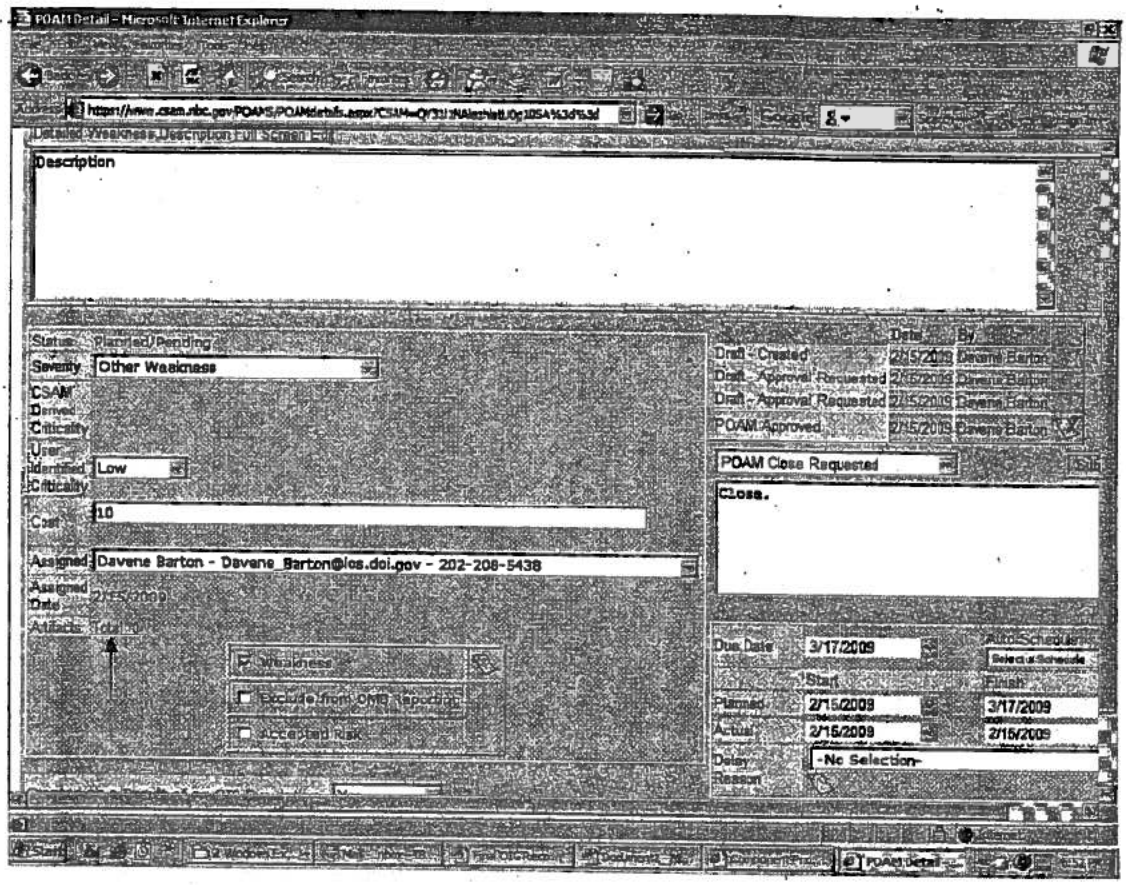


Note: After a POA&M weakness has been closed there are limited capabilities to modify them. Please ensure that newly created POA&Ms are in compliance with this standard. All POA&M weaknesses that are closed but are found to be non-compliant must be corrected or re-created with a reference to the original POA&M ID number in the POA&M Title field. The re-created (new) POA&M must reference the original POA&M ID number in the "POA&M Title" field. Additionally, the original (old) POA&M must reference the re-created POA&M ID number in the "POA&M Title" field.

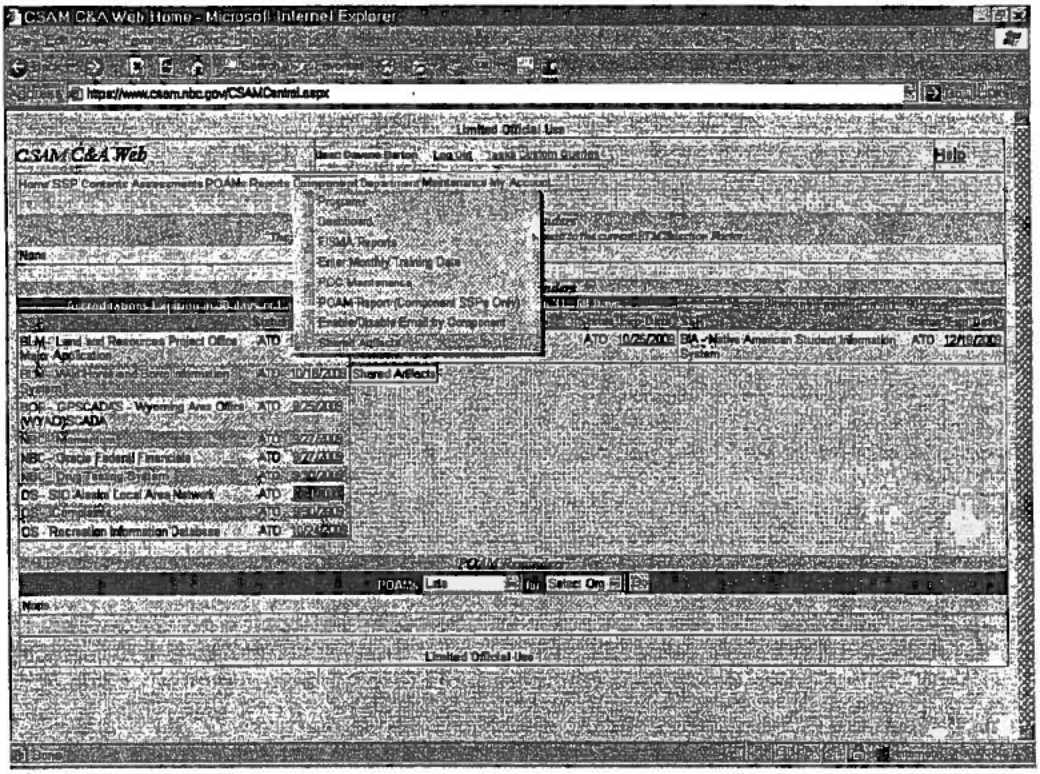
33. Select the paper icon located next to Weakness, Select **Add Comment**, enter the corrective action(s) in the comment field and select **Update**.



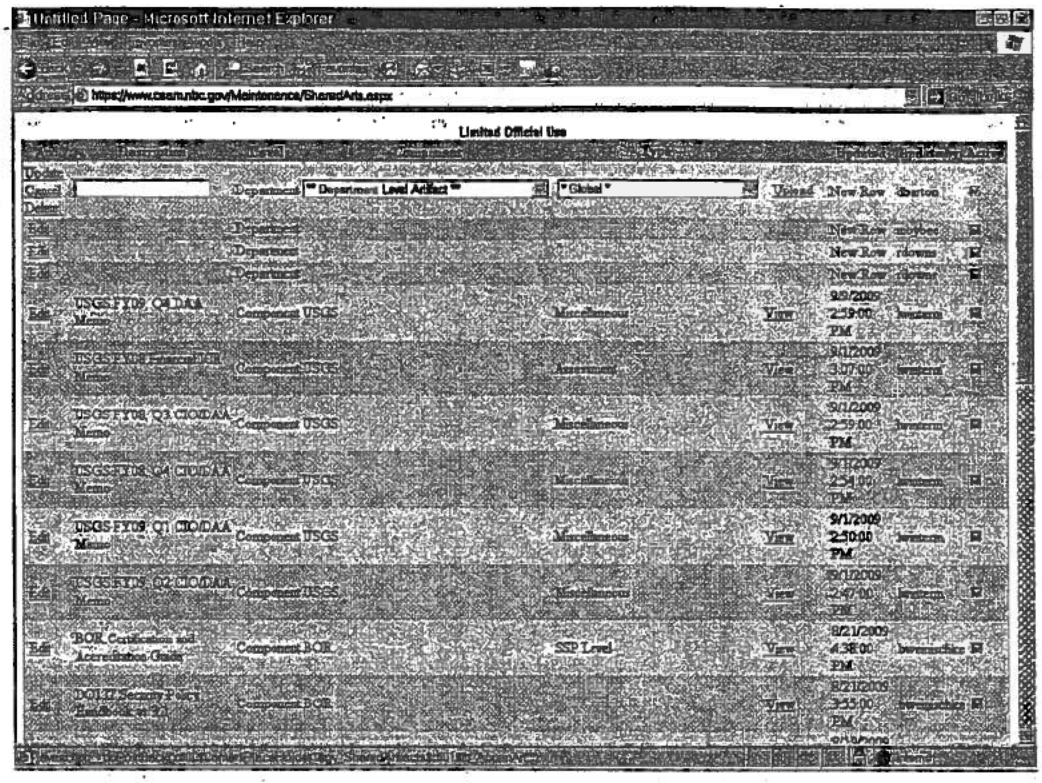
34. Select the Total icon, to the left of Artifacts, upload artifacts such as WCVFs, screenshots, memorandum signature pages and other relevant evidentiary artifacts that clearly demonstrate successful resolution of the weakness.



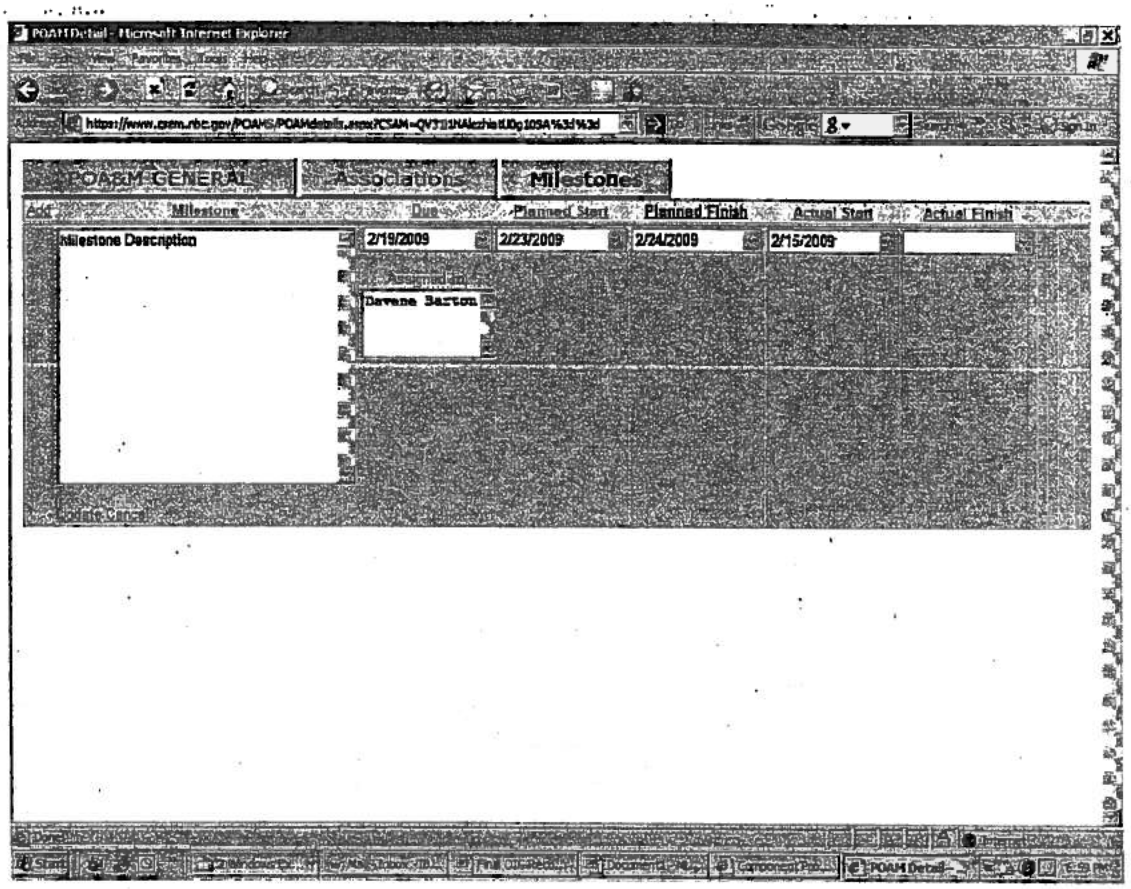
35. To upload CIO and AO Transmittal Memos, return to the home page, select **Component** and then **Shared Artifacts.**



36. Enter artifact **Description**, from the **Component** pick list select bureau or office name, from the **Type** pick list select **Miscellaneous**, select **Upload** to save the information, return to the POA&M module.



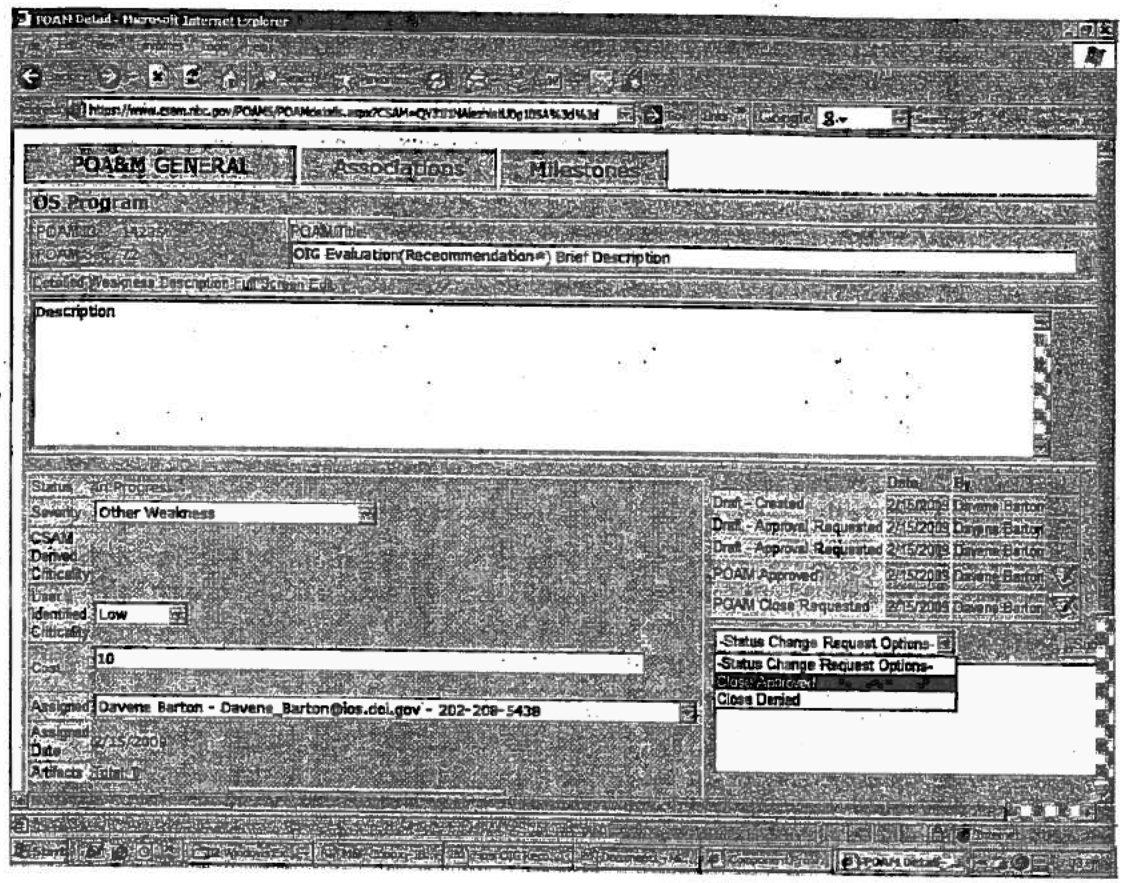
37. Select the **Milestones** tab and then click **Edit**.



38. Enter the milestone **Actual Finish** date.

39. Select **Update** to save the entry and then select the **POA&M General Tab.**

40. Select **Close Approved** from the **Status Change Request Options**, provide comments and then click **Submit**.



41. POA&M Approval Status options.

Draft Created: Each POA&M automatically starts in this state. A POA&M in this state can be deleted by any user who can edit the POA&M

Draft Approve Requested: When the key POA&M information has been entered and finalized, the user responsible for maintaining the POA&M selects this status to request approval. At least one milestone must have been entered before this event can be selected. Requires permission POAMEDIT.

POAM Approved: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been approved. The user responsible for the POA&M can continue carrying out the actions and milestones associated with the POA&M. Once approved, the POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users. Requires permission POAMAPPR or POAMAPSSP.

POAM Approval Denied: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been denied. The user responsible for the POA&M can then make changes and resubmit the approval request. Requires permission POAMAPPR or POAMAPSSP.

POAM Auto Approved: The POA&M will automatically enter this state if it has not already been approved through the manual event process after 90 days from creation. The POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users, with the exception that the Due Date field may be edited once if it was NULL when the POA&M was Auto-Approved.

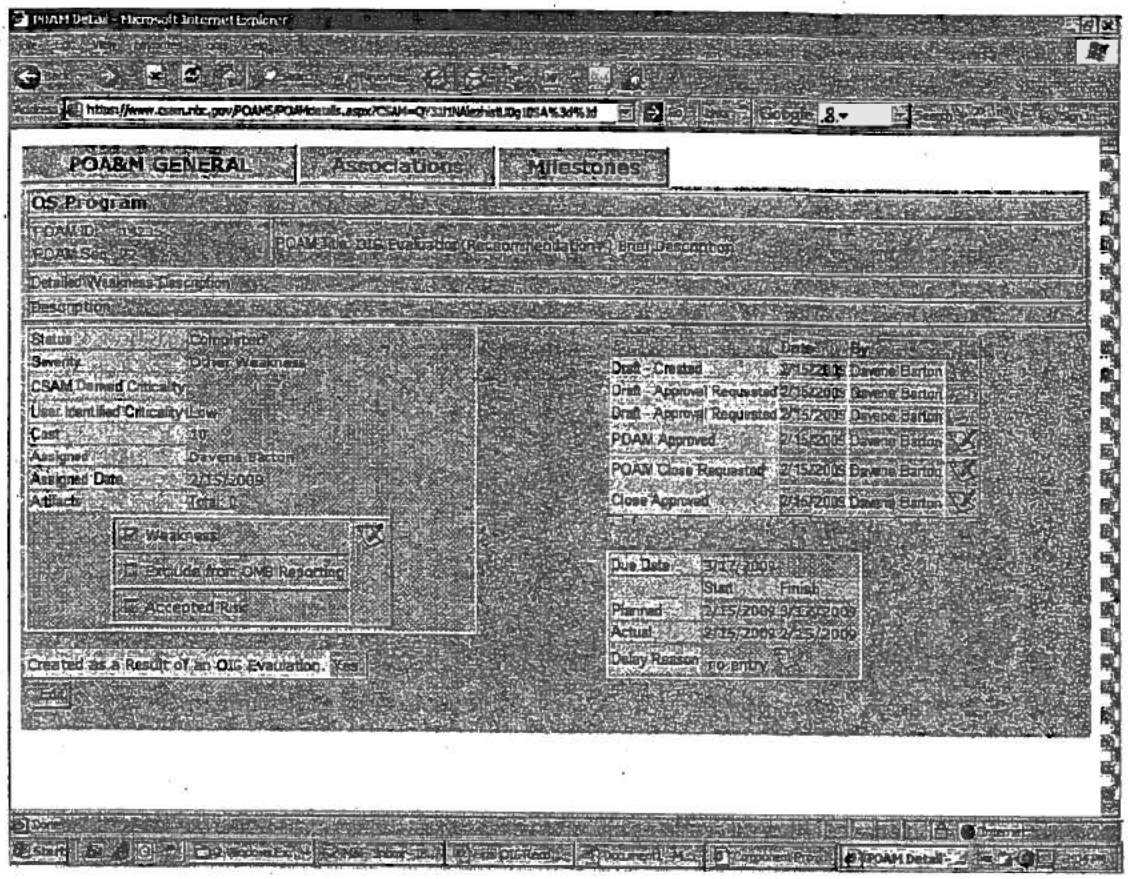
POAM Cancellation Requested: The user responsible for maintaining the POA&M can request cancellation if the POA&M has been approved and is still open. Typically this is done if the POA&M is a duplicate or if the requirement is no longer valid. Requires permission POAMCANCEL.

POAM Close Requested: The user responsible for maintaining the POA&M can request close if the POA&M has been approved and is still open. Typically this is done when after the POA&M actions and milestones have been carried out to completion. The POA&M Actual Start and Actual Finish dates must be populated before this event can be selected. Requires permission POAMCLOSE.

Cancel Approved: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been approved. The POA&M status changes to Cancelled and no further actions are required on the POA&M. Requires permission POAMAPCANCEL.

Cancel Denied: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been denied. The user responsible for the POA&M can then make changes and resubmit the cancellation request with a new justification, or work the actions and milestones to closure. Requires permission POAMAPCANCEL.

42. Enter the **Actual Finish** date and click **Save** to close the POA&M. The status will change from **In Progress, Delayed** or **Ongoing** to **Completed.**



The POA&M Status options are as follows:

Open/Closed: "Open" and "Closed" are not statuses that appear in the Status text field directly, but they are query options ("All Open" and "All Closed"). "All Open" is any POA&M that does not have status Cancelled or Completed. "All Closed" is any POA&M that has status Cancelled or Completed.

Not Started: A POA&M that has no actual start date and is Not Approved.

Planned/Pending: A POA&M that has a scheduled completion date, a planned start, and a planned finish date.

In Progress: A POA&M that has a scheduled completion date, a planned start, a planned finish date, an actual start date, and the POA&M is approved.

Delayed: When a user edits the POA&M, as well as when the nightly procedure executes, the status will be set to "Delayed" status if the POA&M is Approved and past its Due date, but does not currently have a status of "Delayed".

Denied: This is no longer a valid POA&M status. Previously, when the POA&M work flow status was one of the "denied" steps, the POA&M status would also read as "Denied." This was changed to no longer occur in CSAM v2.1. Some POA&Ms may still be in this state at this time if those POA&Ms have not been updated and changed state since the CSAM v2.1 deployment.

Cancelled: The POA&M work flow was moved to Cancel Approved, the POA&M status changes to Cancelled, no further actions are required on the POA&M.

Completed: The POA&M work flow was moved to Close Approved, the POA&M status changes to Closed, no further actions are required on the POA&M.

5 Conclusion

The benefits of the POA&M are significant and far-reaching, internally and externally to DOI. For each system, the POA&M serves as a comprehensive reference to be used in ongoing efforts to address programmatic and system-specific vulnerabilities. The POA&M is an essential management tool for the oversight and mitigation of security weaknesses. To function as an effective tool, POA&Ms must be continually and diligently updated. The operating environment, levels of acceptable risk, and the availability of resources are a small sampling of the many changes that occur on a frequent basis. An effective and successful POA&M document captures each one of these changes in a concise and complete fashion.

Appendix A: References

- Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, V2.0, June 2004.
- National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.[5]
- National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, October 2001.
- National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.*
- National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.*
- Office of Management and Budget Circular A-11, *Preparation, Submission and Execution of the Budget*, (Revised July 25, 2003).
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, November 28, 2000.
- Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.
- Office of Management and Budget Memorandum M-02-09, *Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plan of Actions and Milestones*, July 2, 2002.
- Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003.
- Office of Management and Budget Memorandum M-04-19, *FY 2004 Reporting Instructions for the Federal Information Security Management Act.*
- Office of Management and Budget Memorandum M-05-15 *FY 2005 Instructions for Preparing the Federal Information Security Management Act Report and Privacy Management Report.*
- Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002,* Title III, the *Federal Information Security Management Act of 2002* (FISMA), December 17, 2002.

---

[5] This guidance is in process of revision and will map to NIST SP 800-53 Security Control Categories and provide additional functionality beyond the annual self-assessment.

Appendix B: Acronyms

AO	Authorizing Official
AOSS	All Other Sensitive Systems
BES	Business Essential System
BCISO	Bureau Chief Information Security Officer
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CSAM	Cyber Security Assessment and Management
CSD	Cyber Security Division
CTO	Chief Technical Officer
DAO	Designated Authorizing Official
DOI	Department of the Interior
DOJ	Department of Justice
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FTE	Full Time Equivalent
FY	Fiscal Year
GAO	General Accountability Office
GSS	General Support System
ICR	Internal Control Review
IG	Inspector General
INFOSEC	Information Security
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Major Application
MCS	Mission Critical System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
PUB	Publication
RA	Risk Assessment
SSP	System Security Plan
UPI	Unique Project Identifier
WAN	Wide Area Network
WCVF	Weakness Completion Verification Form

Appendix C: Glossary

Acceptable Risk - a concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.

Adequate Security - security that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Authorizing Official – (formerly known as Designated Approving Authority) official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

Authorizing Official Designated Representative - individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.

Availability - ensuring timely and reliable access to and use of information.

Confidentiality - (1) assurance that information is not disclosed to unauthorized persons, processes, or devices. (2) Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Data Integrity - the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

General Support System (GSS) - an interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data-processing center including its operating system and utilities, a tactical radio network, or a shared information-processing service organization.

Independent Reviewer – is responsible for validating that the corrective action was effectively implemented and that the completion status of the system security weakness has been accurately reported.

Information - any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Owner - is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the

data/information is shared with other organizations. This can be the business owner or in some cases the system owner at DOI.

Information Security (INFOSEC) - protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Information Technology (IT) - any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by DOI whether it is used directly or it is used by a contractor under a contract with DOI which: (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity - (1) the degree to which a system (or system component) prevents unauthorized access to, or modification of, computer programs or data. (2) Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

IT Security Costs - In determining information and IT security costs, Federal agencies must consider the following criteria to determine security costs for a specific IT investment:

1. The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. (Do not include activities performed or funded by the agency Inspector General.) This includes the costs of:

- Risk assessment
- Security planning and policy
- Certification and accreditation
- Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
- Authentication or cryptographic applications
- Education, awareness, and training
- System reviews/evaluations (including security control testing and evaluation)
- Oversight or compliance inspections
- Development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment
- Contingency planning and testing
- Physical and environmental controls for hardware and software

- Auditing and monitoring
- Computer security investigations and forensics
- Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations.

2. Products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; systems administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.
3. Many agencies operate networks, which provide some or all the necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid 'double-counting' agencies should appropriately allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, some agencies find it helpful to ask the following simple question, "If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" Investments that fail to report security costs will not be funded; therefore, if the agency encounters difficulties with the above criteria they must contact OMB prior to submission of the budget materials.

Lead Responder – is responsible for ensuring that project or systems teams have taken appropriate remediation actions or steps to address, partially address, and/or recommend risk acceptance associated with system security weakness.

Major Application (MA) - an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.

Major Information System - a system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should also be evaluated against these criteria. Your agency Capital Planning and Investment Control (CPIC) Process may also define a major system or project. All major systems or projects must be reported on exhibit 53. In addition, a major IT system is one reported on your "Capital Asset Plan and Business Case," Exhibit 300. For the financial management mission area, major is any system that costs more than $500,000. Additionally, if the project or initiative directly supports the President's Management Agenda Items, then the

project meets the criteria of high executive visibility. Projects that are E-government in nature or use e-business technologies must be identified as major projects regardless of the costs. If you are unsure about what systems to consider as major, consult your agency budget officer or OMB representative. Systems not considered "major" are "small/other".

Management Controls - techniques and concerns, normally addressed by an organization's management, that focus on the management of security and risk of an IT system. More expressly, actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions.

Material Weakness - or significant weakness is used to identify control weaknesses that pose a significant risk or threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Operational Controls - procedures and operational methods focusing on mechanisms implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

Plan of Action and Milestone (POA&M) - (a corrective action plan) a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Policy - a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Production System – Any system that stores, processes, or transmits live data or operates in a production environment.

Program Official - a division director or equivalent that is responsible for a major program or functional area.

Program Review - a program review, in the context of the work required under the Government Information Security Reform Act, is a review of the security status of an operational program and is not a security program itself. Each program must be reviewed annually to ensure: 1) risk assessments occur; 2) policies and procedures are risk-based and cost-effective and comply with existing laws and OMB policy; 3) security awareness training for all employees; 4) management testing and evaluation of the effectiveness of information security policies and procedures; 5) a process for remedial action; and 6) procedures for detecting, reporting, and responding to security incidents.

Reportable Condition - A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management. A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations, may be considered a reportable condition. However, due to lower risk, corrective action may be scheduled over a longer period of time. A reportable condition under FISMA is not reported as a material weakness under FMFIA.

Residual Risk – is that risk remaining after all mitigation efforts have been implemented and any other potential corrective action strategies have been exhausted or otherwise determined to be cost-prohibitive when compared to the potential risk impact to the affected information technology system and its associated information/data.

Risk - the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur.

Risk Assessment - the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Risk Management - the total process of identifying, controlling, and remediating information system-related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Security - technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Also referred to IT Security.

Security Controls - the management, operational, and technical controls (i.e., safeguards or countermeasures), prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.

Security Program - a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems.

Sensitive Data - information whose loss, misuse, unauthorized access to, modification, or destruction, could adversely affect the national interest or the conduct of Federal programs, or privacy to which individuals are entitled, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy, etc. Sensitive data can relate to industry (e.g., proprietary, patented), copyrighted or business data, as well as data that is simply inappropriate for public release.

Sensitivity - the degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components.

Significant Deficiency - is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA).

System - a collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected. (Defined in NIST SP 800-16, Appendix C). A system can also be defined as the interconnected set of information resources under the same direct management control, which share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Technical Controls - automated, technological security mechanisms the IT system executes. The controls can provide automated protection for unauthorized access or misuse and facilitate detection of security violations.

Technical Reviewer – is responsible for ensuring that project or system team have taken appropriate remediation actions or steps to address, partially address, and/or recommend risk acceptance associated with the system security weakness. The technical reviewer is also responsible for ensuring all appropriate Security Technical Implementation Guide (STIGs) have been updated as noted.

Vulnerability - a flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Appendix D: Weakness Completion Verification Form

Completing Corrective Actions

In order to implement a needed security control and 'complete' a weakness, five levels of effectiveness must be met as follows:

1. The control objective must be documented in a security policy (e.g., the policy can either be a common control where the policy has been promulgated at the Departmental or bureau level, a system-specific policy issued as a rules of behavior (ROB) to users, etc.);
2. The security control must be documented as procedures (e.g., documented procedures, practices, security configuration guides (STIGs), etc.);
3. Procedures have been implemented;
4. Procedures and security controls are tested and reviewed; and
5. Procedures and security controls are fully integrated into a comprehensive program.

Three examples of appropriate corrective actions follow.

- **Management Control** - If the identified weakness was a lack of management controls (e.g., policies or standards), an appropriate corrective action might be development of a relevant and appropriate IT security policy. Adequate evidence that the corrective action was completed would be demonstrating that a final version of the policy was approved, signed, and promulgated by the responsible senior management official and disseminated and effectively communicated to individuals within the organization that needed to be informed and/or trained about the policy.

  It may also be necessary to implement or update related operational and/or technical security controls consistent with the policies or standards developed to fully correct the identified weakness. Even though a security audit, test, or assessment failed to specifically identify these additional follow-on steps, the System Owner and other individuals responsible for the security of a system must take appropriate steps to identify any such additional activities and document on the POA&M by creating new POA&M entries, or by adding additional milestones to the existing related weakness, and then continue to implement corrective actions until all aspects of the weakness are addressed.

- **Operational Control** - If the identified weakness was a lack of operational controls (e.g., procedures, practices, or Security Technical Implementation Guides (STIGs), an appropriate corrective action might be implementation of operational practices and procedures that are consistent with established and relevant IT security policies and standards. Adequate evidence that the corrective action was completed would be demonstrating that a final version of documented procedures exists and those responsible offices and individuals have been identified and have begun to effectively implement those practices.

  It may also be necessary to implement or update related technical security controls consistent with existing policies or standards to support and help ensure efficient and

effective operational procedures and practices. Although the operational control should be able to demonstrate that it is compliant with a related management control, existence of the management control (although required) is not sufficient evidence that an operational control exists. Adequate evidence would include documented procedures and practices and evidence that implementation has been at least initiated by responsible offices and individuals.

- **Technical Control -** If the identified weakness was a lack of technical controls (e.g., security patches, operating system, application, database, web-services security configurations consistent with applicable STIGs, encryption of sensitive data or passwords, ineffective identification, authentication, or access controls, insufficient audit logging of security events, etc.), an appropriate corrective action might be implementation of appropriate device security configurations that corrects or mitigate the weakness, in a manner that is consistent with established and relevant IT security policies, standards, procedures, and practices.

  Evidence that the corrective action was completed would be documentation of change records and associated approvals and completion signatures or other audit trails, results from independent vulnerability scanning tests using similar tools and methods of initial discovery, results from independent manual review of security configurations following similar inspection criteria and methodology used in initial discovery, etc. Although the technical control should be able to demonstrate that it has been implemented in a manner that is compliant with a related management control, existence of the management control (although required) is not sufficient evidence that the technical control exists, has been implemented correctly, and has been tested for effectiveness.

Weakness Completion Verification Form

The Weakness Completion Verification Form is embedded in the following logo.

Final WCVF Template
17 Mar 10.doc

Appendix E: POA&M Certification Transmittal

This section contains the templates of the Certification Transmittals to be completed by the CIO and AO and submitted as part of the quarterly POA&M submission.

The CIO Certification Transmittal is embedded in the following logo.

CIO Transmittal Memo Template.doc

The AO Certification Transmittal is embedded in the following logo.

AO Transmittal Memo Template.doc

Appendix F: Office of Inspector General Recommendation Status Reporting Process

Introduction

The Office of Inspector General (OIG) Information Security Division (ISD) conducts regular evaluations of IT security related functions throughout Interior. As IT security weaknesses are discovered the OIG generates reports to relay their recommendations to the affected bureaus and offices as well as to the Department's Office of the Chief Information Officer (OCIO).

All bureaus and offices must ensure that all OIG recommendations have a corresponding Plan of Action and Milestone (POA&M) in the Cyber Security Assessment and Management (CSAM) application. Bureaus and offices are required to provide quarterly updates in CSAM with a detailed status of remediating actions with regard to all open OIG recommendations since fiscal year 2007. In lieu of the adhoc process established in 2008 where bureaus and offices submitted their quarterly reports via word documents, effective FY 2009 Quarter 1, the updates must be entered into CSAM. The OIG will review POA&Ms created as a result of their evaluation in CSAM to make sure weaknesses are incorporated. The findings will be reviewed no less than quarterly to evaluate the effectiveness of corrective actions.

Within the OCIO, the Cyber Security Division (CSD) POA&M and Audit Liaison service area has been charged with the responsibility of providing oversight of the remediation actions by bureaus and offices as well as Departmental offices.[6] In performance of CSD's oversight function, the CSD shall act as the central point of contact for reviewing, providing feedback, and tracking status of bureau, office, and Departmental updates to the OIG.

Purpose

The purpose of this document is to define a process by which the OCIO CSD shall coordinate the reporting of detailed resolution status of OIG recommendations on a quarterly basis. This document describes the methodology by which the POA&M and Audit Liaison shall collaboratively:

- Ensure bureaus and offices are aware of the deadlines for status reporting;
- Periodically review bureau and office updates in CSAM;
- Provide feedback to the bureaus and offices regarding required data elements.

Bureau/Office Responsibilities

[6] *Departmental Manual, Part 18, Paragraph 18.5(A) 1* requires the Department's "Information Technology Security Staff" to perform oversight.

Bureaus and offices are responsible for responding to each of their respective OIG report recommendations by creating a POA&M in CSAM. POA&Ms created as a result of an OIG evaluation must remain open until the CSD has the opportunity to re-evaluate them and confirms they are resolved to their satisfaction.

If the weakness has been remediated, enter the corrective action description as a milestone, change the **Status Change Request Option** to **Closure Requested** and upload evidentiary artifact(s) that demonstrate successful resolution (See Section 5, **POA&M Management** for more information on how to create and manage POA&Ms). Once the CSD has re-evaluated the POA&M weakness and determined that the weakness has been resolved to their satisfaction, the Bureau Chief Information Security Officer (BCISO) will be notified via e-mail from the CSD.

FISMA §3544(a) 2 requires policies and procedures to cost effectively reduce risk and periodically test information security controls to ensure they are effectively implemented. The Inspector General Act (as amended) §2 requires the OIG to promote economy, efficiency, and effectiveness. The purpose of requiring all OIG information security findings to be recorded in CSAM as a POA&M and require these POA&Ms to remain open until the CSD affirms they are resolved is to establish a procedure for ensuring the OIG's recommendations are addressed.

Bureaus and offices must also upload evidentiary artifacts in all updates whether the recommendation remains open or is closed. The CSD and OIG verifies accomplished milestones and progress in remediating weaknesses and require supporting evidence to do so. In addition to the Weakness Completion Verification Form (WCVF), at least one artifact that supports closure of the recommendation must be uploaded for every OIG recommendation that bureaus and offices have referenced as closed. Artifacts can be e-mails, screen shots, procedure documents etc., as long as the artifact provides sufficient and relevant detail to enable the OIG to conduct testing and/or evaluation of the effectiveness of the corrective actions taken.

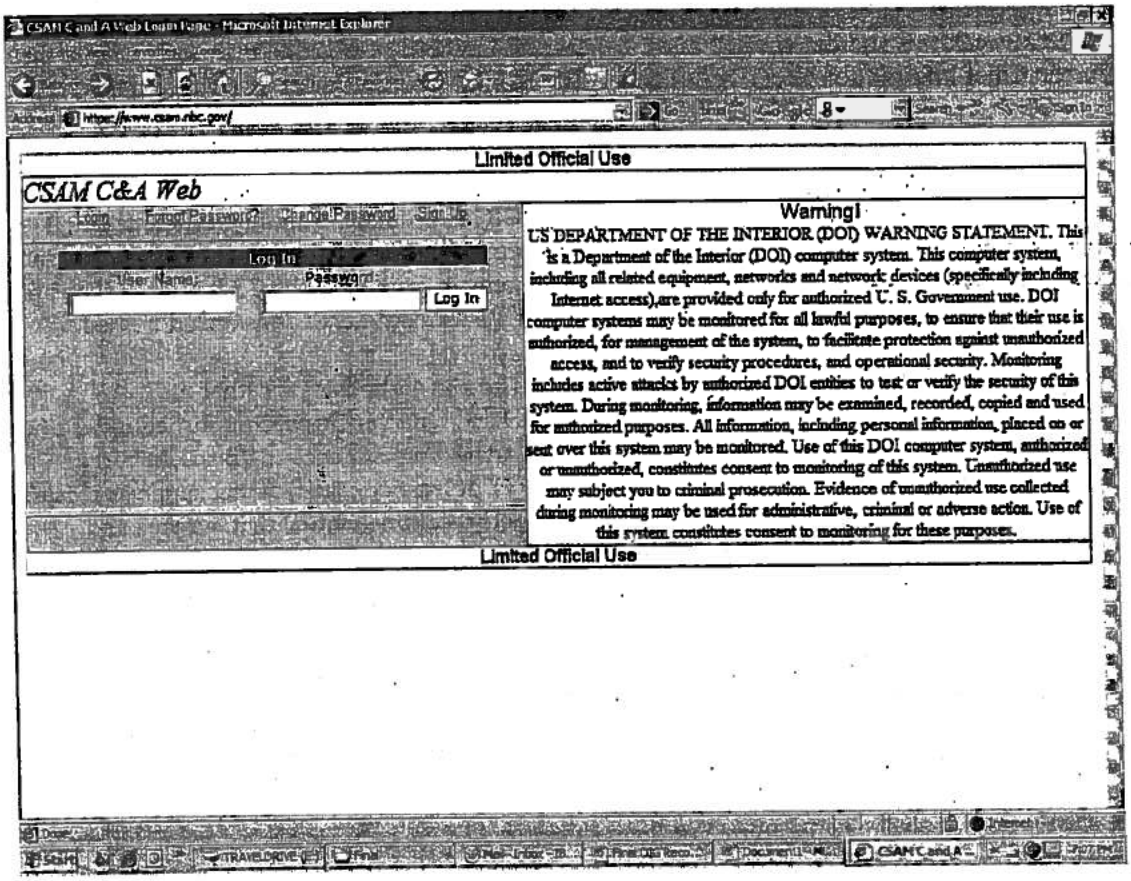
Reporting Schedule

Please refer to Section 2.8.2, Managing and Monitoring Progress.

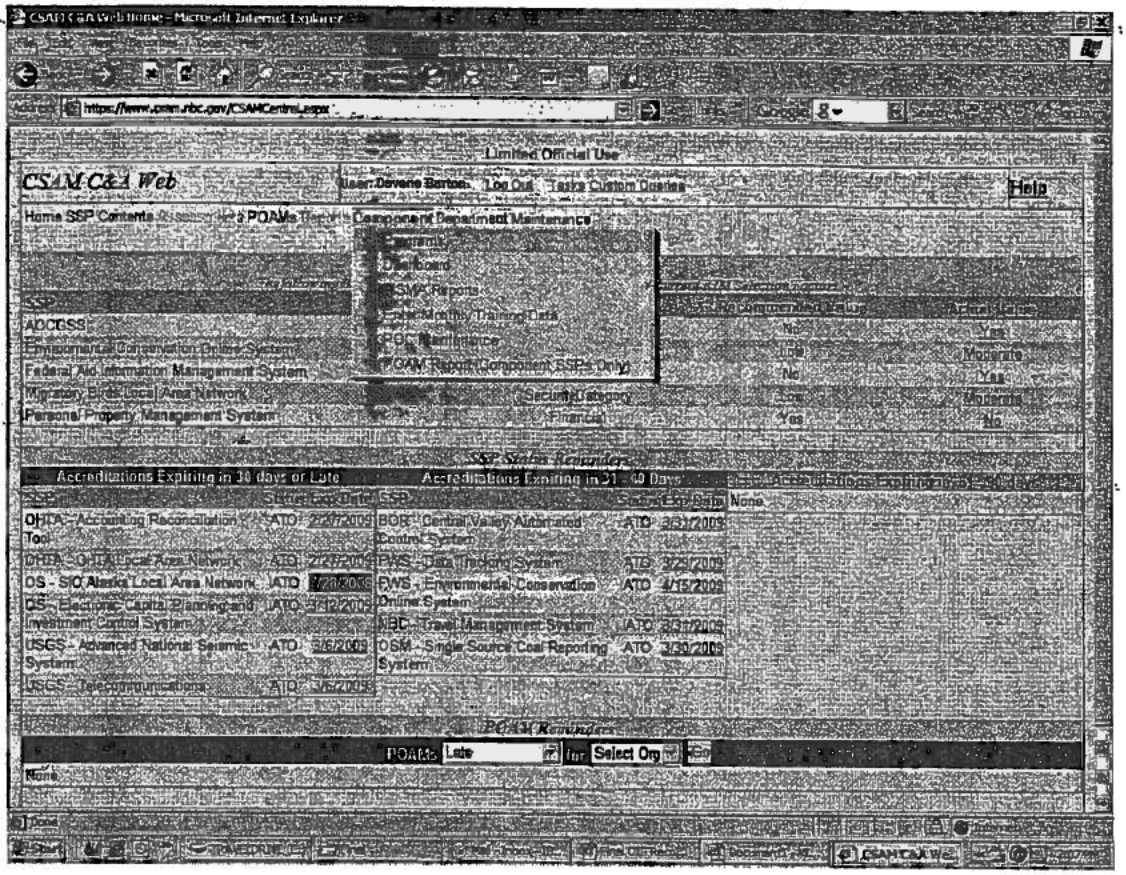
Creating and Managing POA&Ms

This section will explain how to create and manage program and system POA&Ms as a result of an OIG evaluation in CSAM.

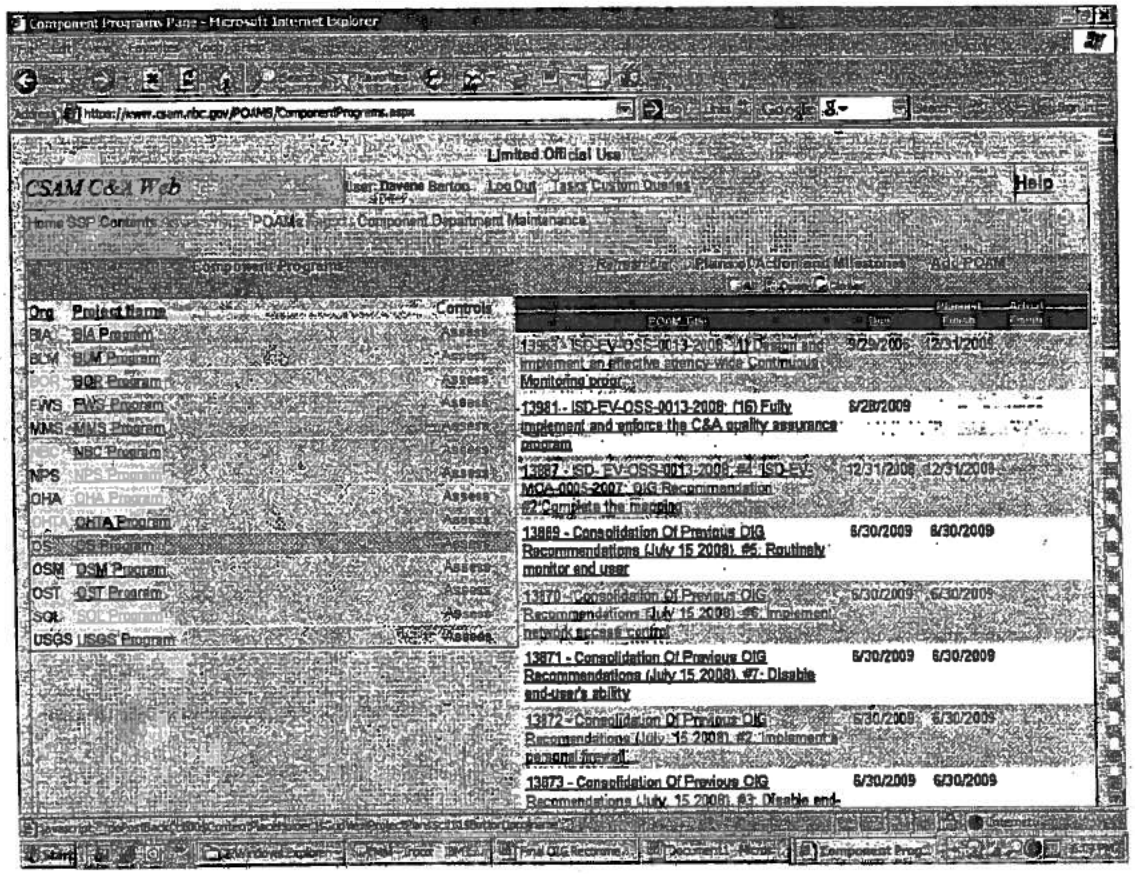
1. To create a program or system POA&M go to: https://www.csam.nbc.gov.
2. Enter your User Name and Password and then select **Log in.**



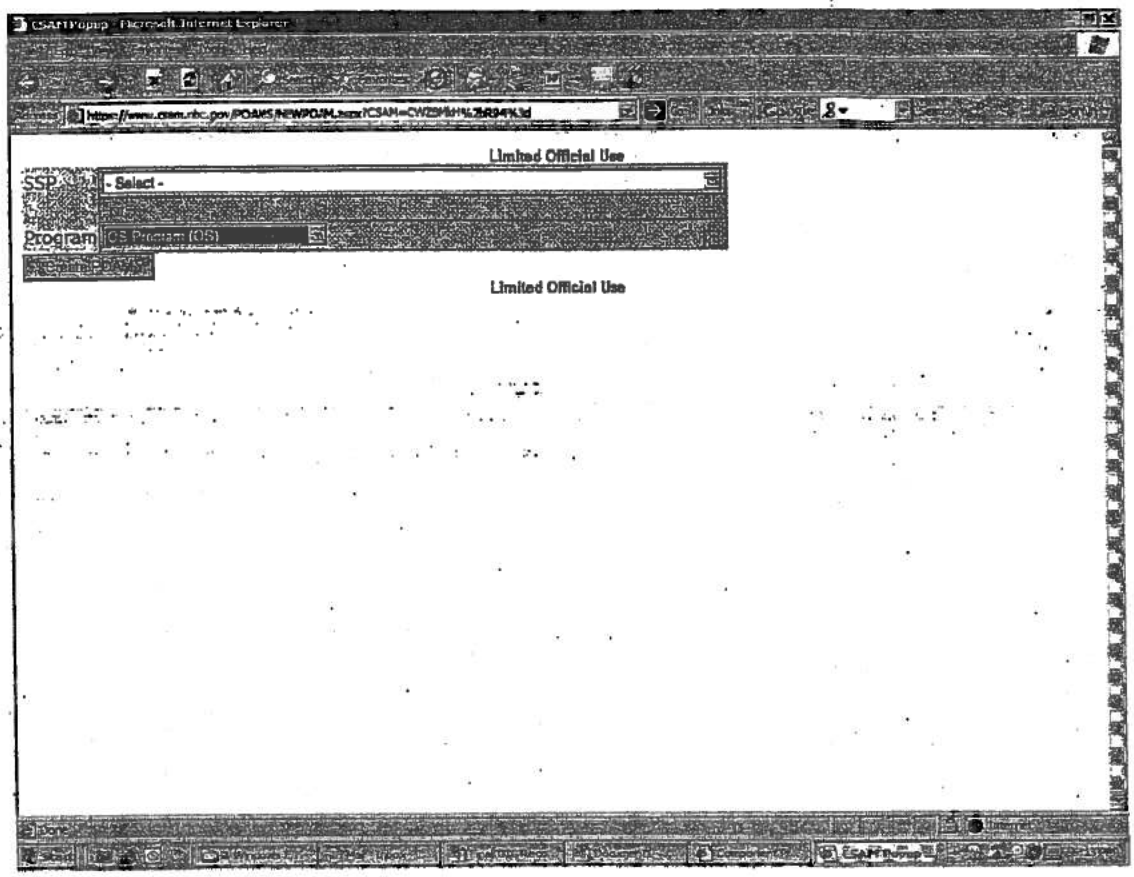
3. Select the **Component** link and the select the **Programs** link.



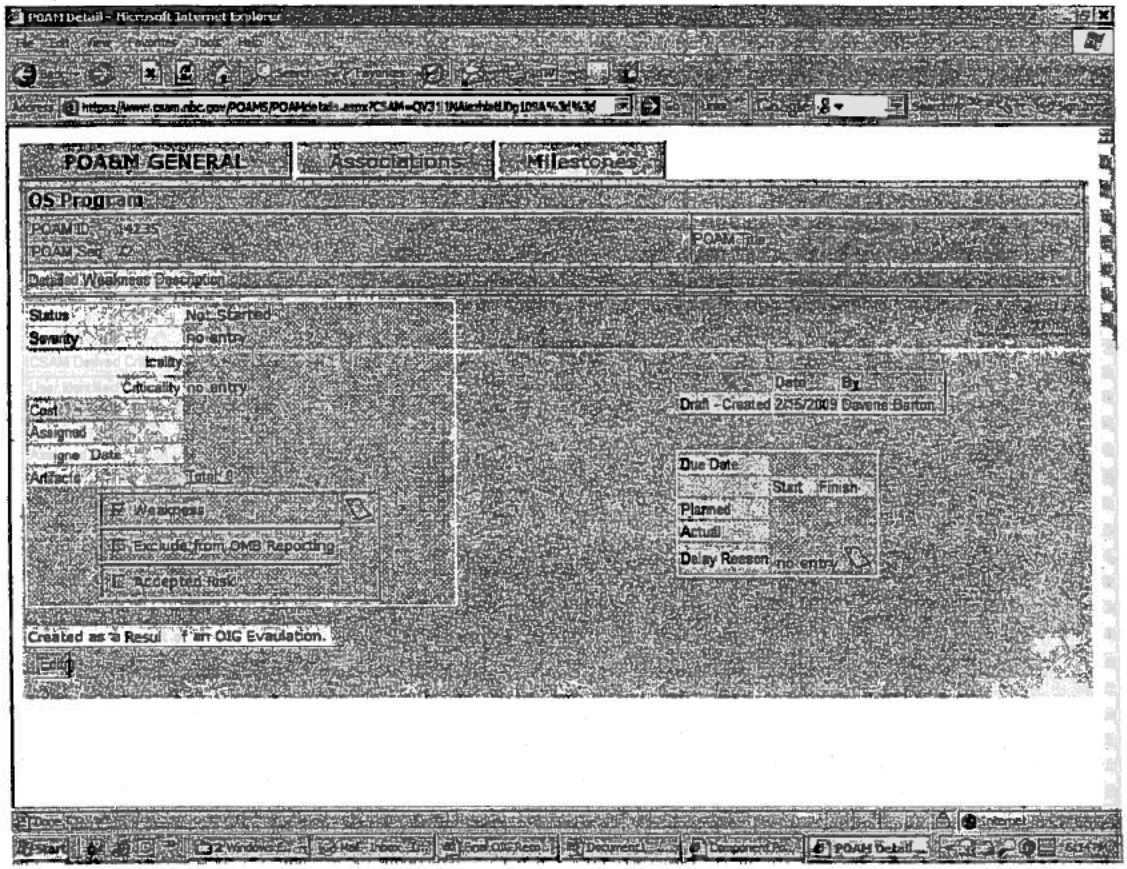
4. Select your bureau/office **Project Name** and then click the **Add POA&M** button located on the right side of the screen.



5. Select the **Program** or **SSP** (system) name from the pick list and then select **Create POA&M**. (Note: Users will only have access to the systems/program specific to their bureau or office).

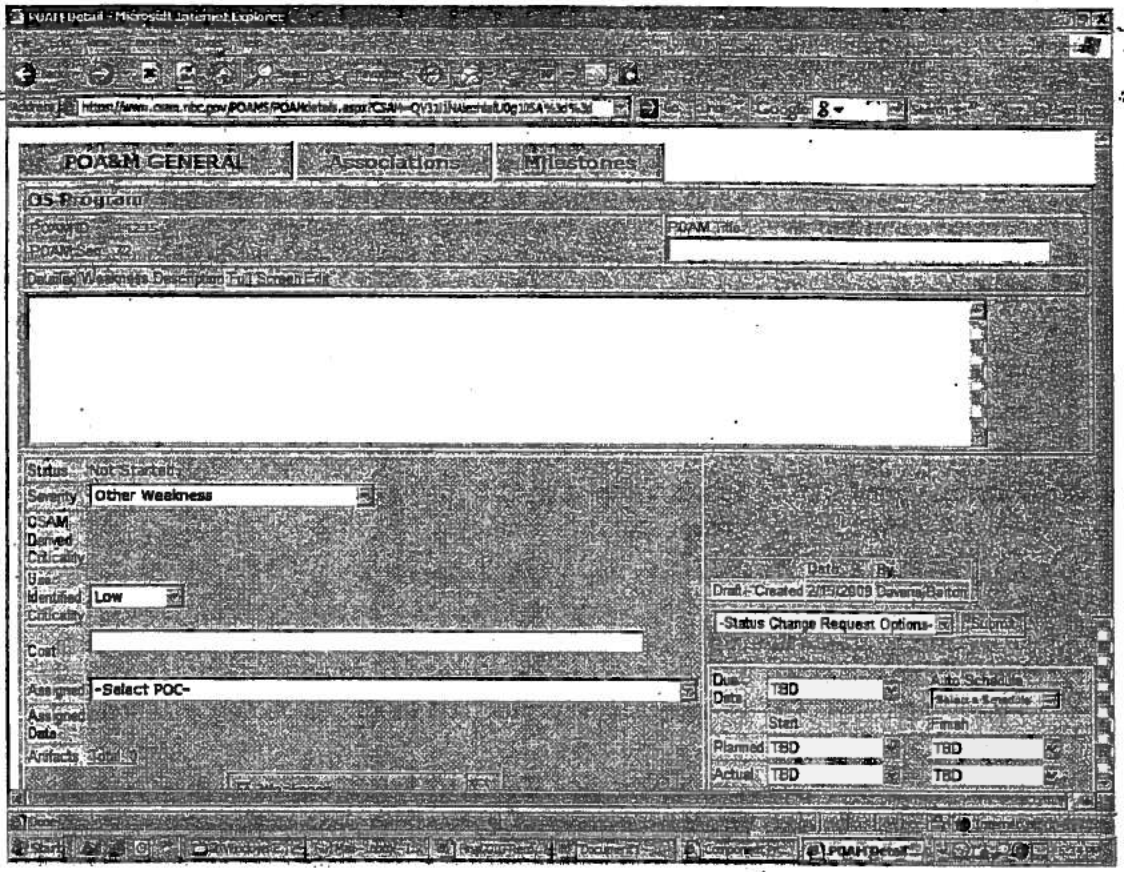


6. Select Edit.



The **POA&M ID** is a CSAM generated unique number for each POA&M. This number is unique amongst all system, site and program POA&Ms.

The **POA&M Seq.** is a CSAM generated unique number for each POA&M. This number is unique only within the system, site or program it belongs to. This number is sequentially assigned.

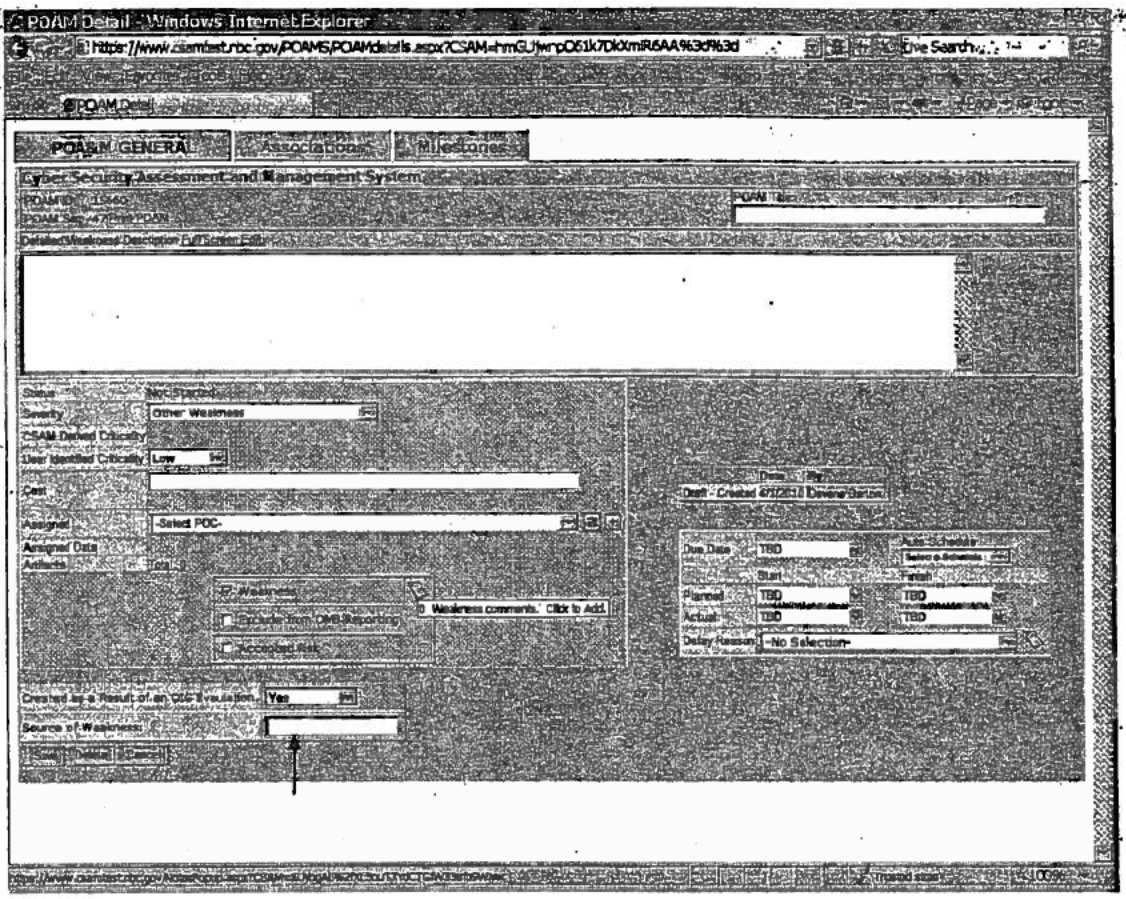


7. Enter **POA&M Title.** Enter the OIG report evaluation number the recommendation number and a brief description of the weakness Select **Edit** Select **Edit.**
8. Enter **Detailed Weakness Description. Enter the detailed weakness description in the text box using the exact language identified in the OIG report evaluation.** (Note: If the OIG recommendation has been identified in multiple reports, open only one POA&M and list all report evaluation numbers and recommendation numbers).
9. Enter **Severity** by clicking the drop- down menu and choosing the applicable option.
10. **CSAM Derived Criticality.** CSAM automatically ranks the criticality of a POA&M when the vulnerability is associated at the Control or Expected Results level and is unaware of the operating environment of the system (i.e., is not aware of any mitigating/compensating controls that would justify any lower risk rating – e.g., a vulnerable port/service might have an initial risk rating of high but when taking into consideration an external firewall that prevents any other system from accessing the vulnerable port/service the user identified risk level might be adjusted to medium or low).

    The **CSAM Derived Criticality** value is dynamically updated as the associated control implementation status changes. In the event the vulnerability is not associated at the

control or expected result level, the user identified criticality level must be populated. An example of this may be Program related vulnerabilities.

11. Select the **User Identified Criticality** of the POA&M from the pick list. Using data from a user defined risk assessment process, enter appropriate the criticality level. (Note: The User Identified Criticality level is the "official criticality level" to the extent that it is selected/identified as instructed by this POA&M Process Standard. If it is not adjusted by the user then the "official criticality level" would default to the "CSAM Derived Criticality".
12. Enter the **Cost** information. POA&M cost can be captured and associated with the POA&M, providing visibility on several other CSAM screens. This capability enables IT Security Specialists and management to make credible, risk-based decisions with regard to the operation and use of information systems.
13. Enter **Assigned POC.** This assignment is made from a drop down table of POCs for which CSAM contains contact information online.
14. Enter the **Due Date** also known as the Schedule Completion Date (SCD). This date is the key date that will be locked-down as the baseline, once the POA&M is approved. While in Draft POA&M status, this value can be changed. The user can also enter dates directly into individual fields. Auto-scheduler sets the **Due Date, Planned Start** and **Planned Finish** dates, however, the user must enter the **Actual Start** and **Actual Finish** dates manually.
15. Select **Yes** from the **Created as a Result of an OIG Evaluation** pick list, enter the **Source of Weakness. When entering the source of weakness information bureaus/offices must include the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness.** Click **Save.**



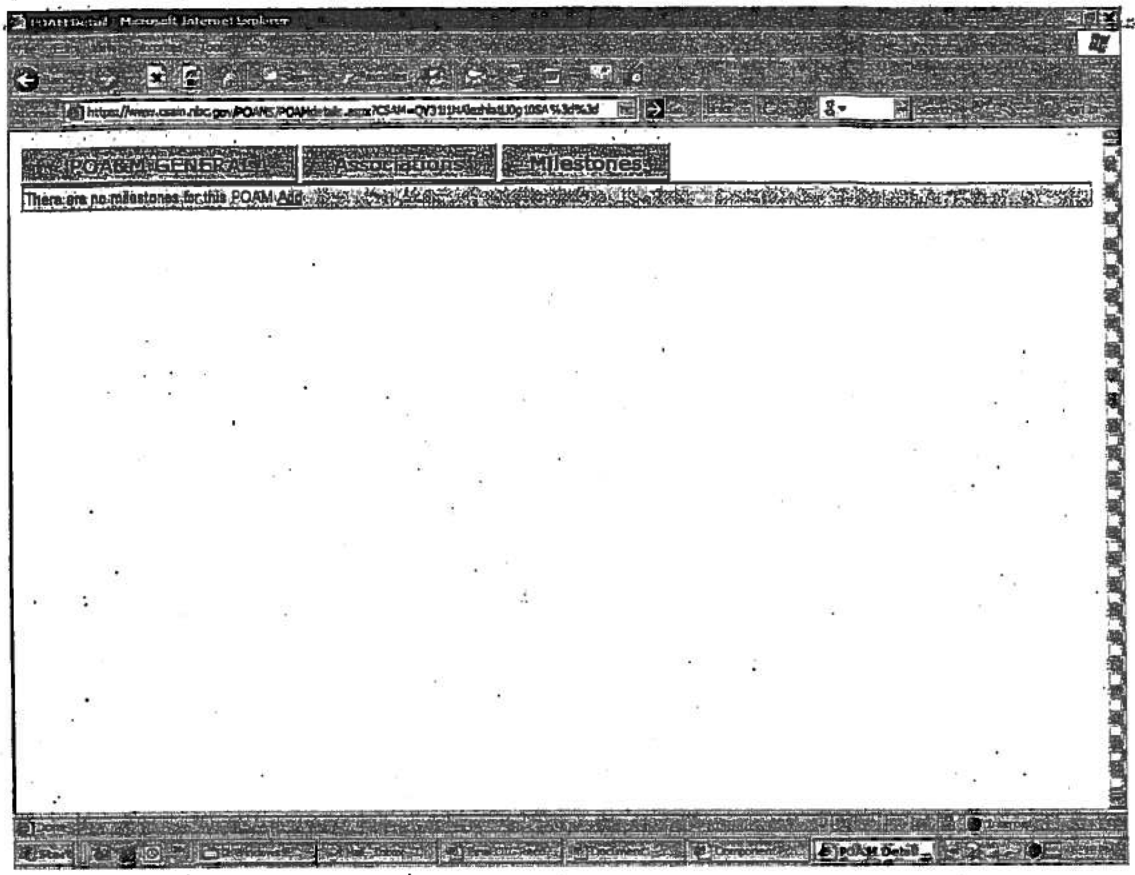
Note: *Given existing constraints, and the capabilities of the current version of CSAM, the only options available in the system to record the source of weaknesses other than those identified by the OIG are by entering that information as part of the POA&M Title, the POA&M Detailed Weakness Description, or as a User Defined Attribute (UDA).*

As Interior believes adding an additional discrete field clearly designated for the identification of "Source of Weakness" within CSAM would be beneficial to all participating agencies we have submitted a change request for consideration and, if approved, will implement that change as part of the planned scheduled release of the new upgrade version as soon as it becomes available.

In the interim, CSD has created a User Defined Attribute (UDA) labeled "Source of Weakness" that is now an attribute of every POA&M weakness within CSAM. While CSAM will continue to maintain the existing DOI-specific UDA labeled as "Created as a Result of an OIG Evaluation" having a value of either "Yes" of "No" to enable the OIG to identify all POA&M weaknesses that are associated with OIG report findings and recommendations, the new "Source of Weakness" UDA provides a text field with a sufficient number of types of permissible characters for bureaus/offices to identify all

sources of weaknesses by including the auditing entity, the title of the report, the report number, the date of the report, the specific finding and/or recommendation of the report, and any other information pertinent to the source of the weakness. It is anticipated that this interim approach will enable Interior to more easily migrate the information in the temporary UDA fields to the more permanent fields following DOJ's implementation of the change request (expected to take at least six months or longer – DOJ is unable to provide any specific commitments and/or dates at this time).

16. Select the Milestones tab:



The key milestones associated with each corrective action should be identified on each POA&M. Each weakness must have one or more associated milestones. Milestones should define the major steps that will be performed to complete the corrective action. If there is more than one milestone, list and number each milestone in the order they should be executed. For example, one set of milestones for a weakness such as, "Identification and authentication are not adequate for the level of security controls required for this system" might be:

1) Evaluate methods for strengthening identification and authentication.

2) Recommend solution and obtain approval.

3) Develop procedures to standardize accepted identification and authentication process.

4) Design identification and authentication solution.

5) Build identification and authentication solution.

6) Test identification and authentication solution.

7) Deploy identification and authentication solution and implement supporting process.

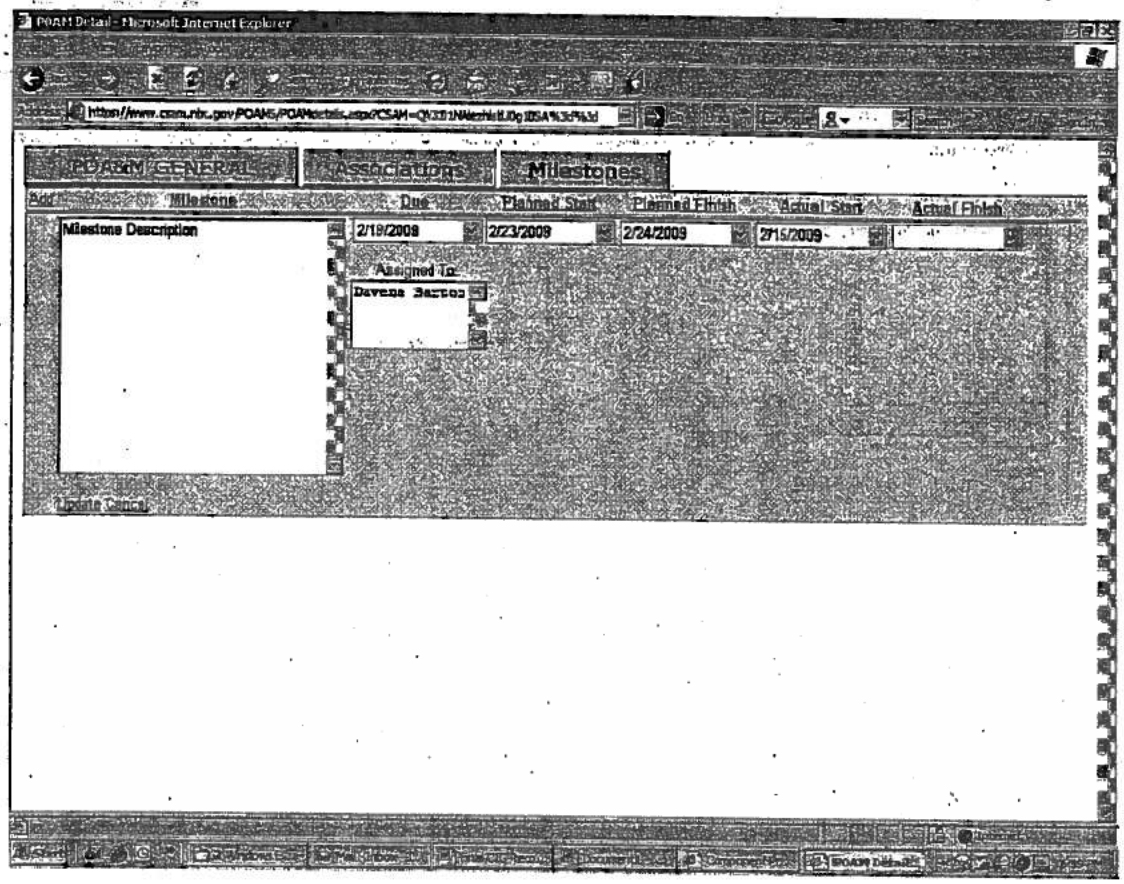
Milestones might also include more specific aspects related to the technical solution (e.g. implement two-factor authentication), and management and operational controls related to the steps for implementing supporting business practices and procedures where additional security control requirements are known or anticipated.

The description of each milestone must be detailed enough so that an independent reviewer will understand the planned corrective action and determine whether the corrective action is adequate and appropriate and will result in the weakness being corrected or its associated risk mitigated to a level acceptable to the AO. Sensitive information can be included as needed for the description since the entire POA&M is a sensitive but unclassified document.

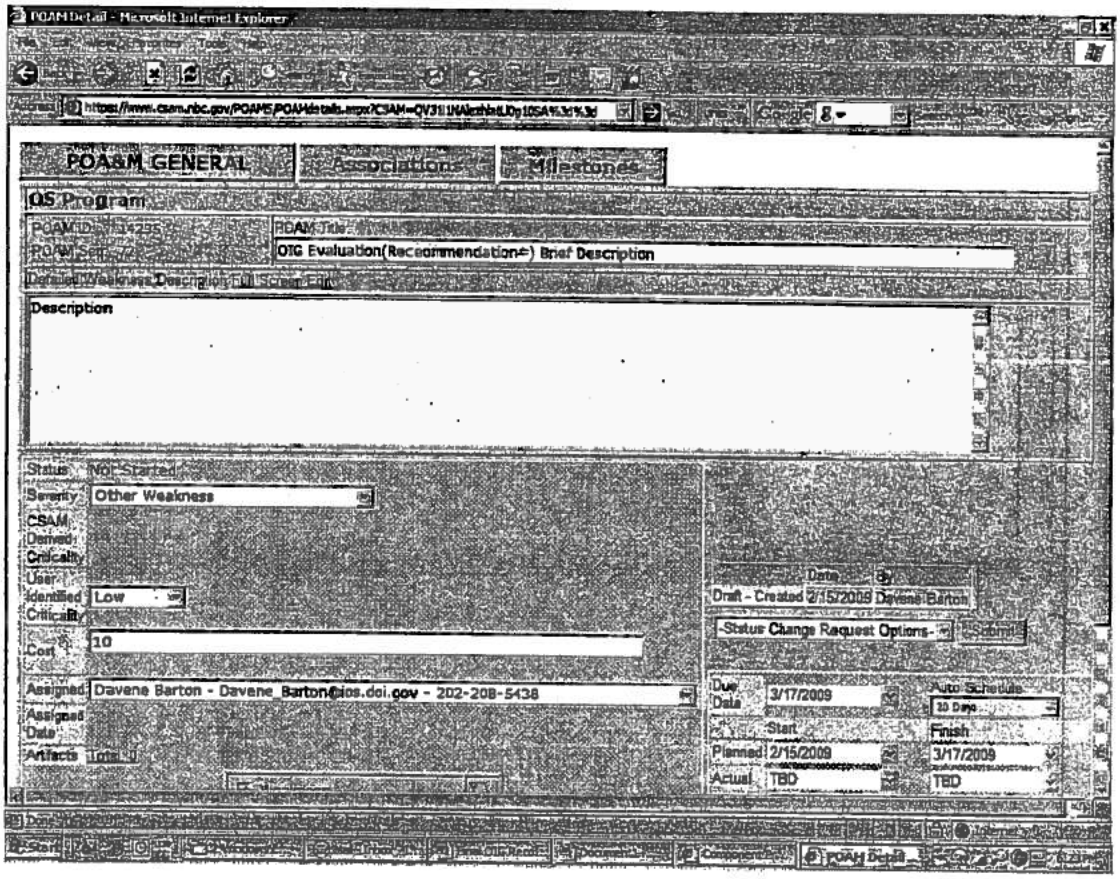
Milestones should start with planned remediation actions, show progression through remediation and/or must be updated periodically or as remediation actions occur.

Milestones should always end in a statement clearly indicating completed remediation action; Entries of TBD, N/A, and similar responses indicating future tense, proposed or intended actions are not compliant.

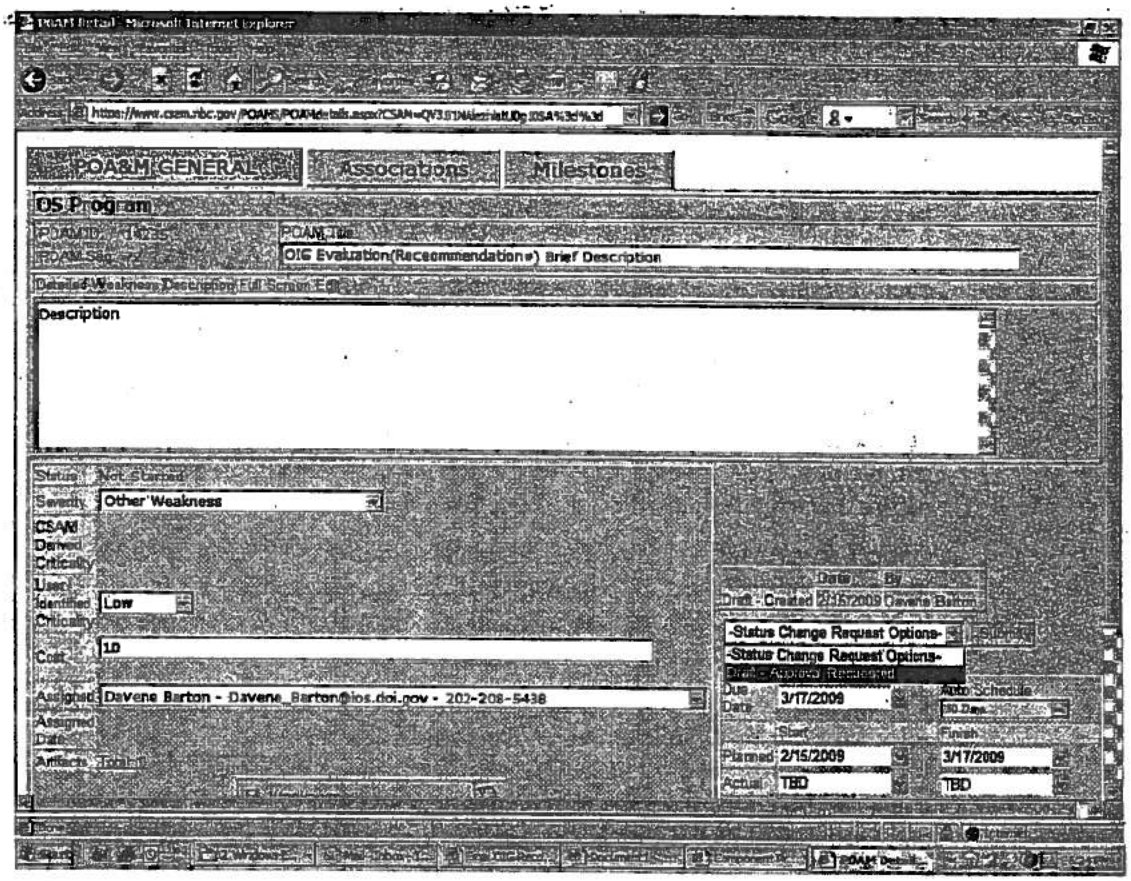
17. Select **Add** to add a milestone and enter required dates. At least one milestone must be added before a POA&M can be approved.
18. Select **Update** to save the entry.



19. Select the **POA&M General** tab and then select **Edit.**



20. Select **Draft – Approval Requested** from the **Status Change Request Options** pick list and then click **Submit**.



The POA&M Approval Status options are as follows:

Draft Created: Each POA&M automatically starts in this state. A POA&M in this state can be deleted by any user who can edit the POA&M

Draft Approve Requested: When the key POA&M information has been entered and finalized, the user responsible for maintaining the POA&M selects this status to request approval. At least one milestone must have been entered before this event can be selected. Requires permission POAMEDIT.

POAM Approved: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been approved. The user responsible for the POA&M can continue carrying out the actions and milestones associated with the POA&M. Once approved, the POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users. Requires permission POAMAPPR or POAMAPSSP.

POAM Approval Denied: The user responsible for reviewing POAM Approval requests selects this status to indicate that the request has been denied. The user

responsible for the POA&M can then make changes and resubmit the approval request. Requires permission POAMAPPR or POAMAPSSP.

POAM Auto Approved: The POA&M will automatically enter this state if it has not already been approved through the manual event process after 90 days from creation. The POA&M Title, Detailed Weakness Description, and Due Date fields are locked in read-only mode for regular users, with the exception that the Due Date field may be edited once if it was NULL when the POA&M was Auto-Approved.

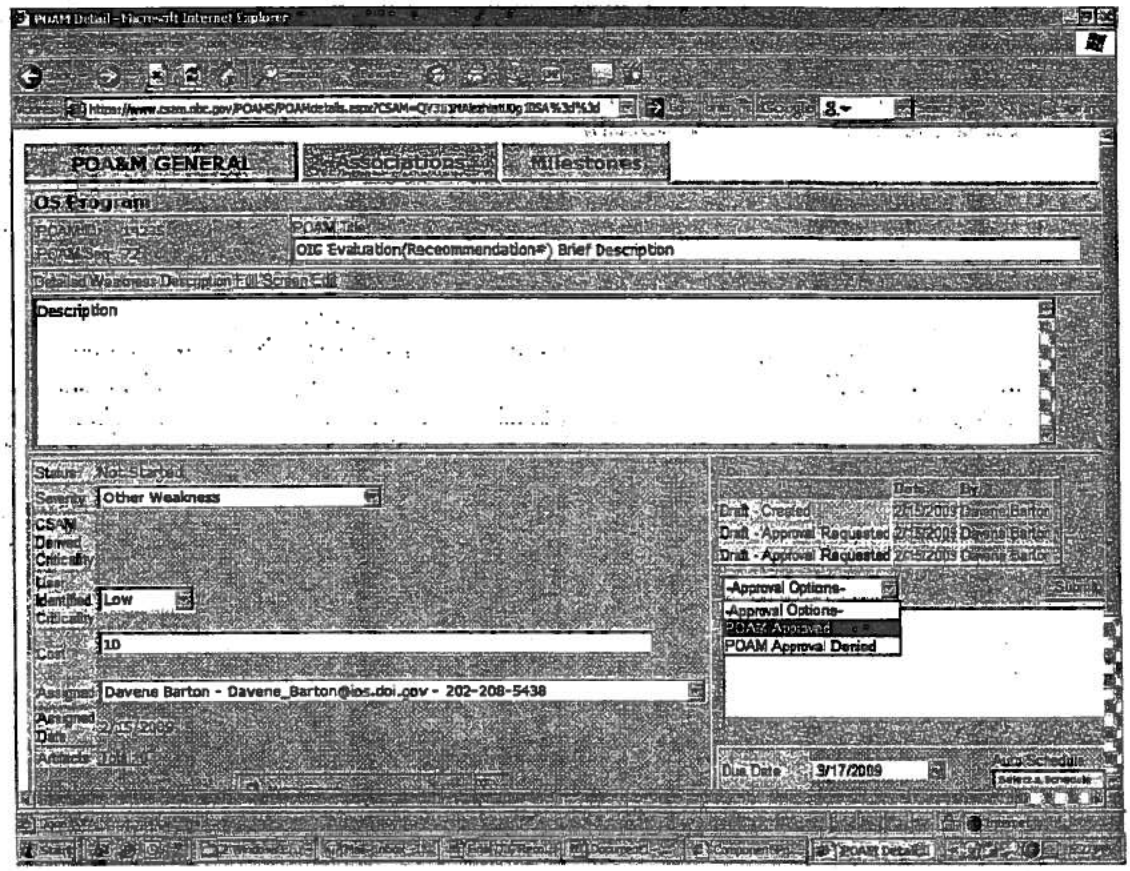
POAM Cancellation Requested: The user responsible for maintaining the POA&M can request cancellation if the POA&M has been approved and is still open. Typically this is done if the POA&M is a duplicate or if the requirement is no longer valid. Requires permission POAMCANCEL.

POAM Close Requested: The user responsible for maintaining the POA&M can request close if the POA&M has been approved and is still open. Typically this is done when after the POA&M actions and milestones have been carried out to completion. The POA&M Actual Start and Actual Finish dates must be populated before this event can be selected. Requires permission POAMCLOSE.

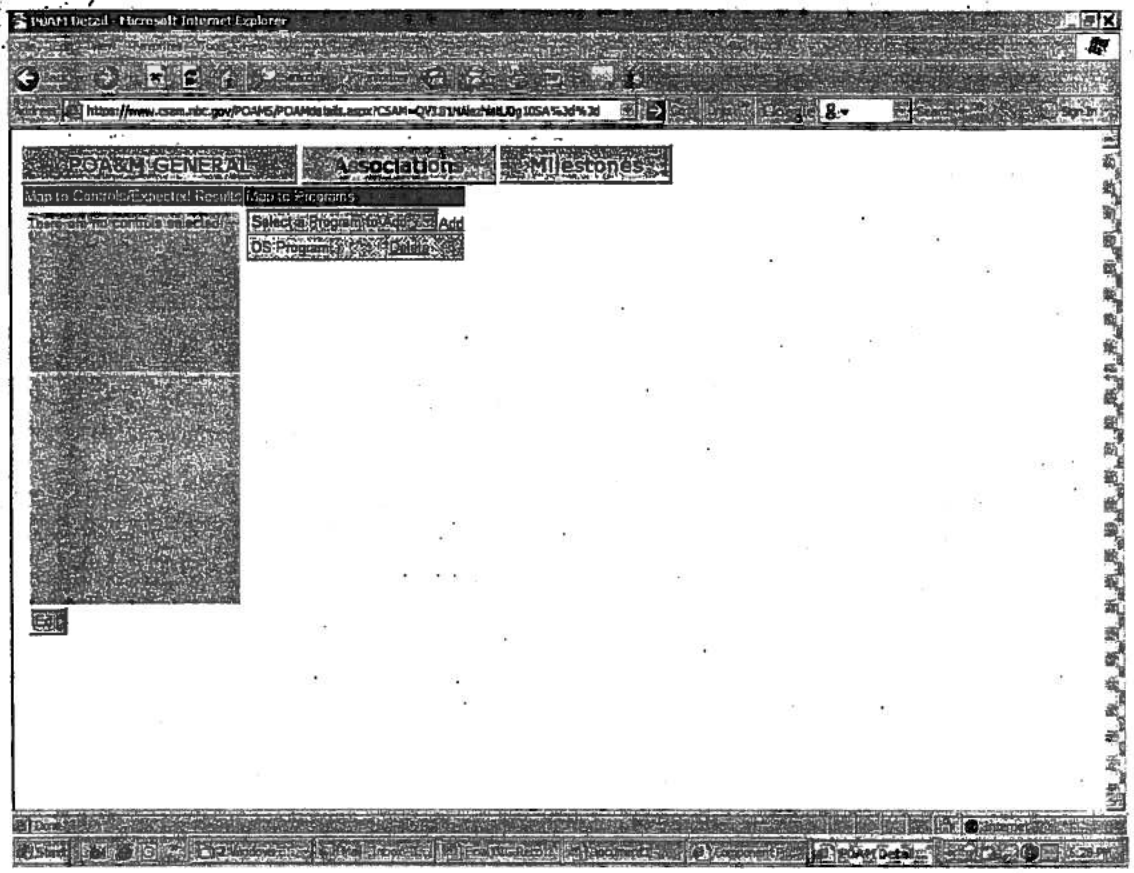
Cancel Approved: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been approved. The POA&M status changes to Cancelled and no further actions are required on the POA&M. Requires permission POAMAPCANCEL.

Cancel Denied: The user responsible for reviewing POAM Cancellation requests selects this status to indicate that the request has been denied. The user responsible for the POA&M can then make changes and resubmit the cancellation request with a new justification, or work the actions and milestones to closure. Requires permission POAMAPCANCEL.

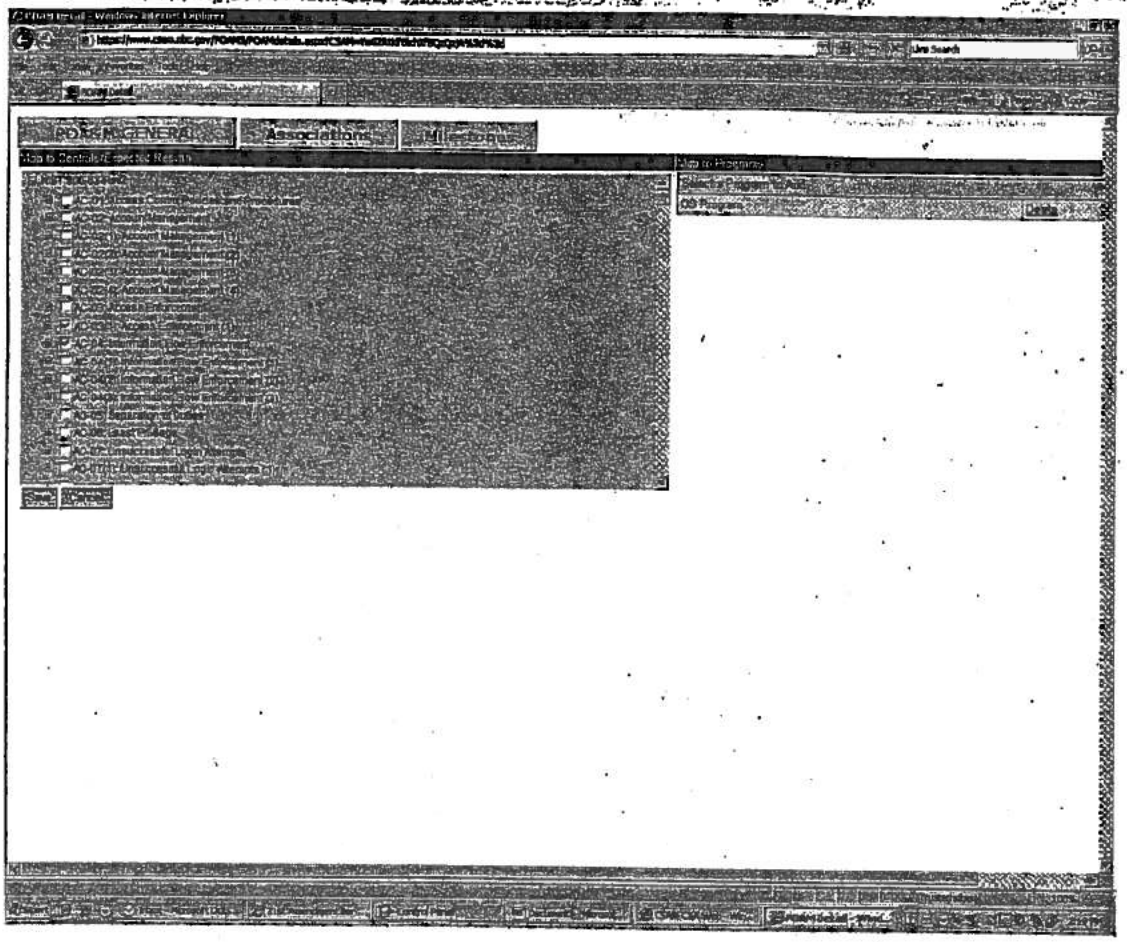
21. To approve entry of the POA&M, From the POA&M General tab select **Edit, POA&M Approved** from the **Status Change Request Options**, provide comments and then click **Submit**.



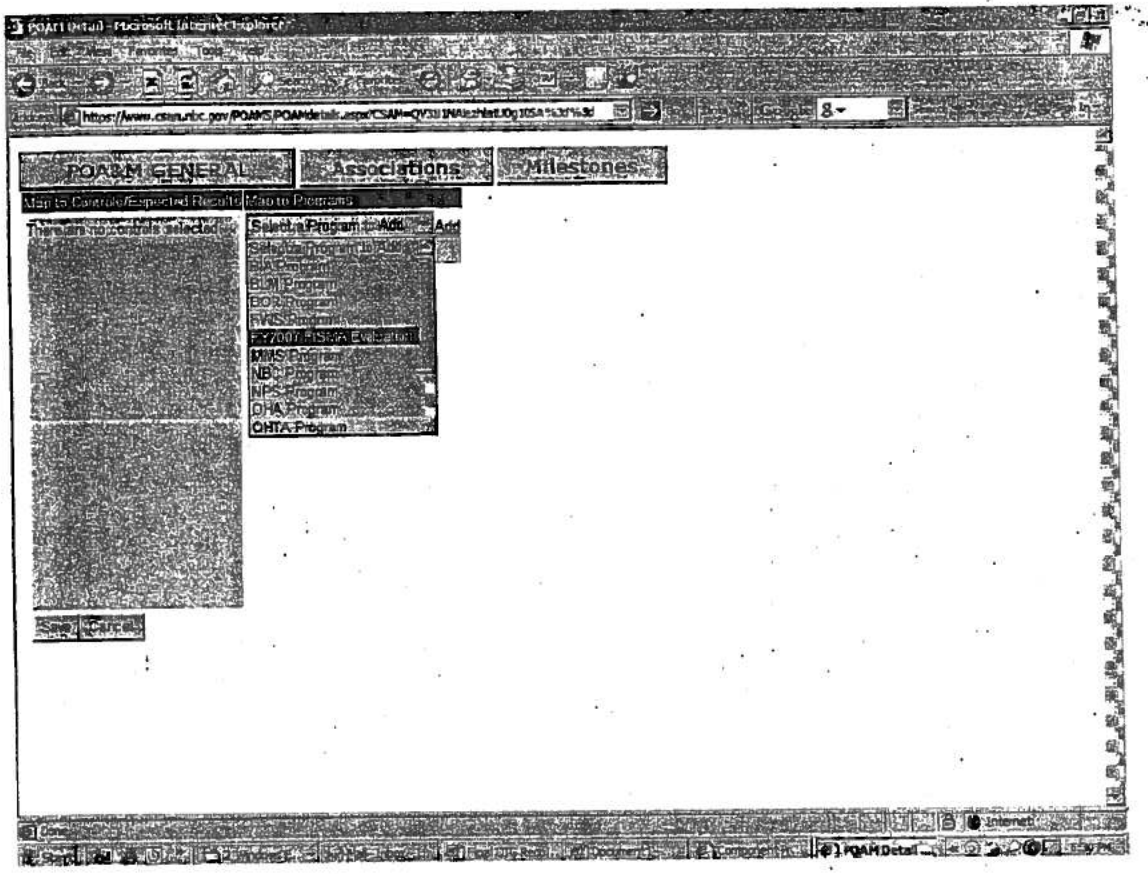
22. Select the **Associations** tab to tag multiple controls and expected results to Programs.



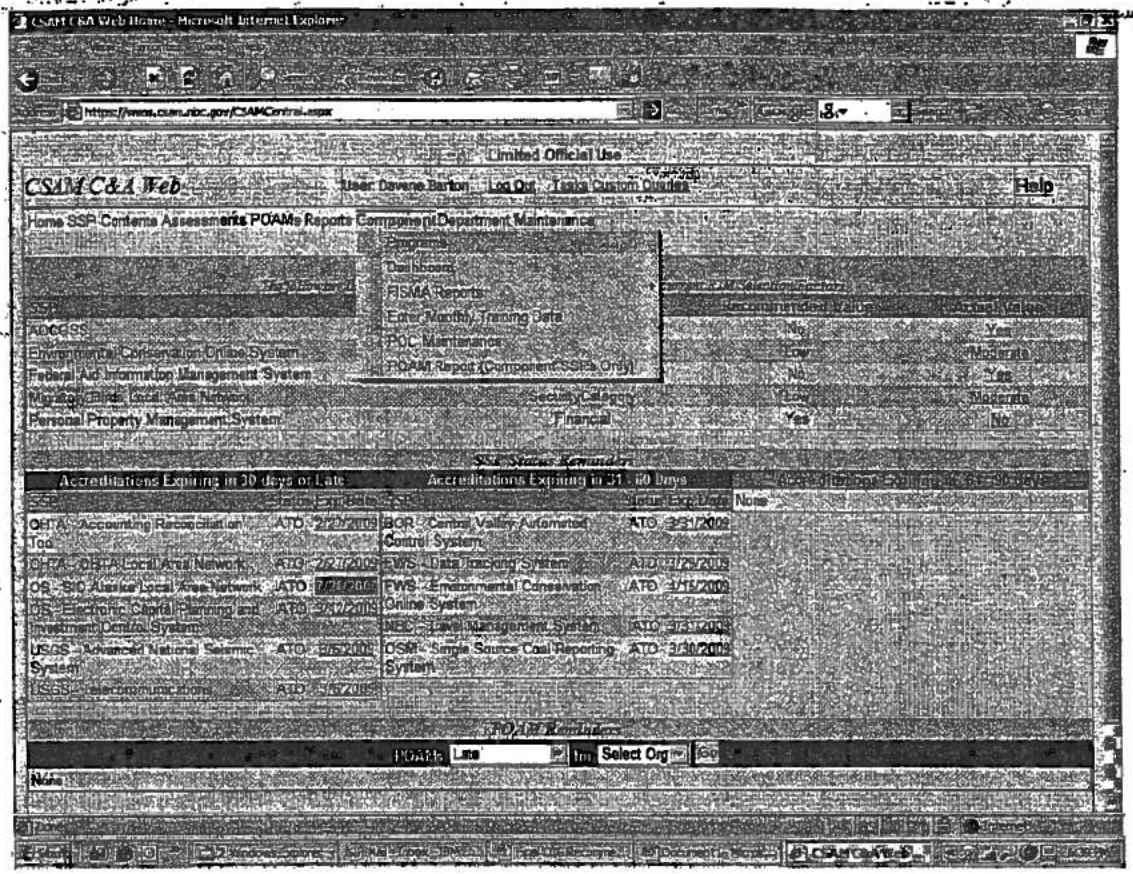
23. Select **Edit**.
24. Select applicable controls.



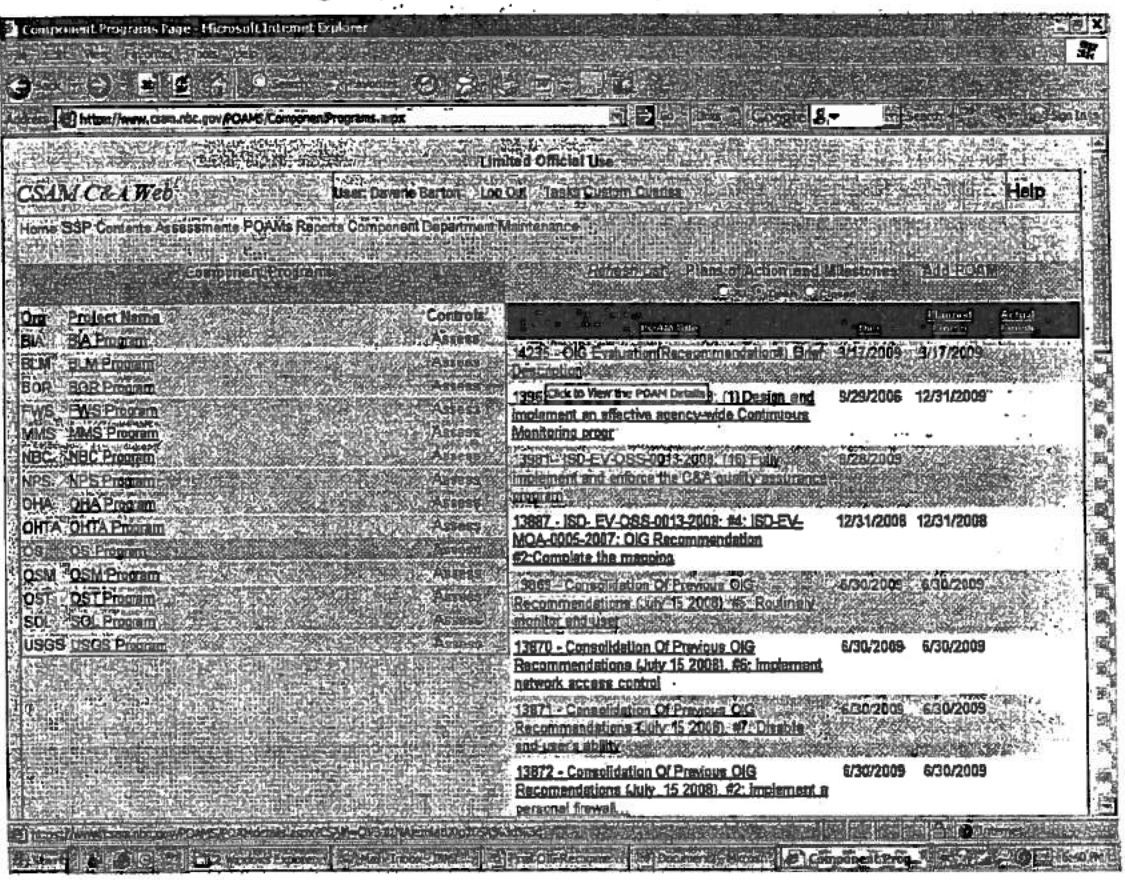
25. Select a Program to add and then click **Add.** (Note: Please map POA&Ms created as a result of an OIG evaluation to the appropriate "FY200X FISMA Evaluation" program and then click **Save.**
26. Select the **POA&M General** Tab and exit the application. This completes the POA&M creation work flow process.


POA&M GENERAL
Associations
Milestones
Map to Controls/Expected Results
Map to Programs
There are no controls selected
Select a Program to Add
Add
BLM Program
BOR Program
FY2007 FISMA Evaluation
MMS Program
NBC Program
NPS Program
OHA Program
OHTA Program
Save
Cancel

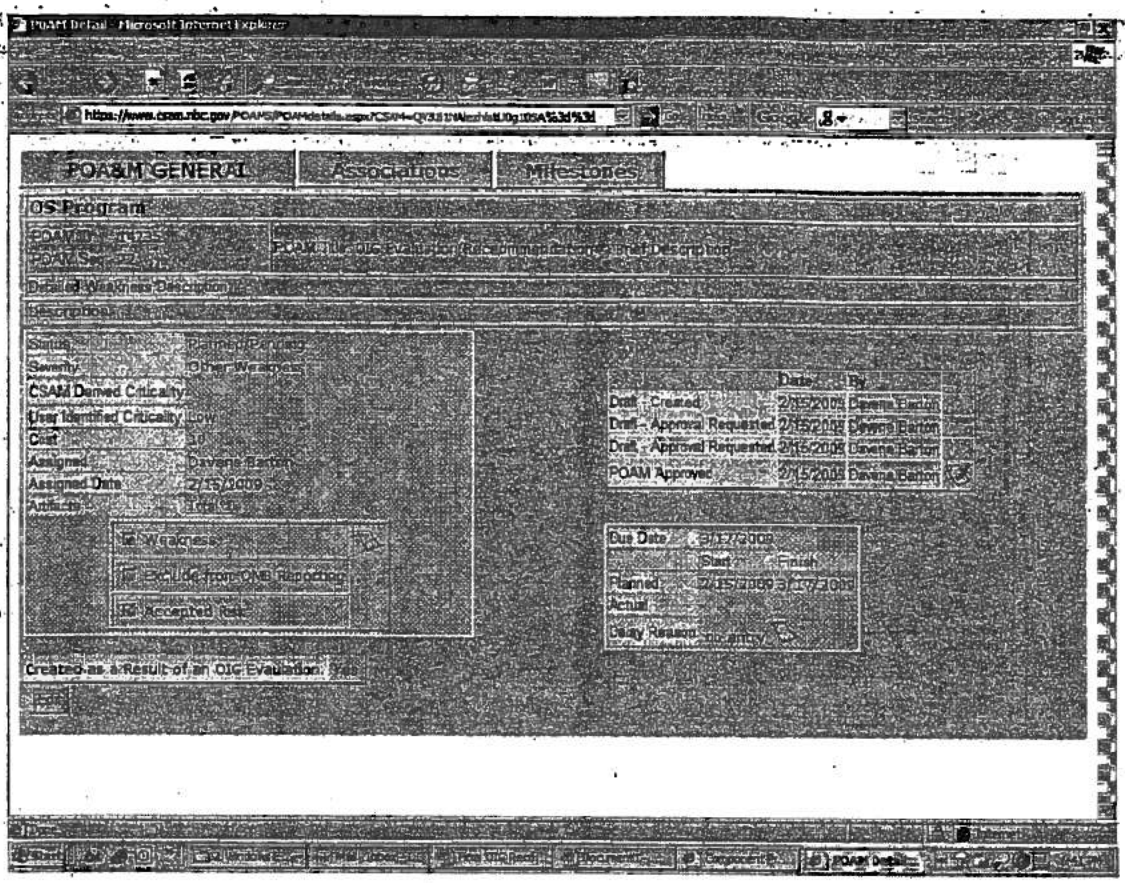
27. To request closure of a POA&M, select the **Component** link and then scroll down and select the **Programs** link.



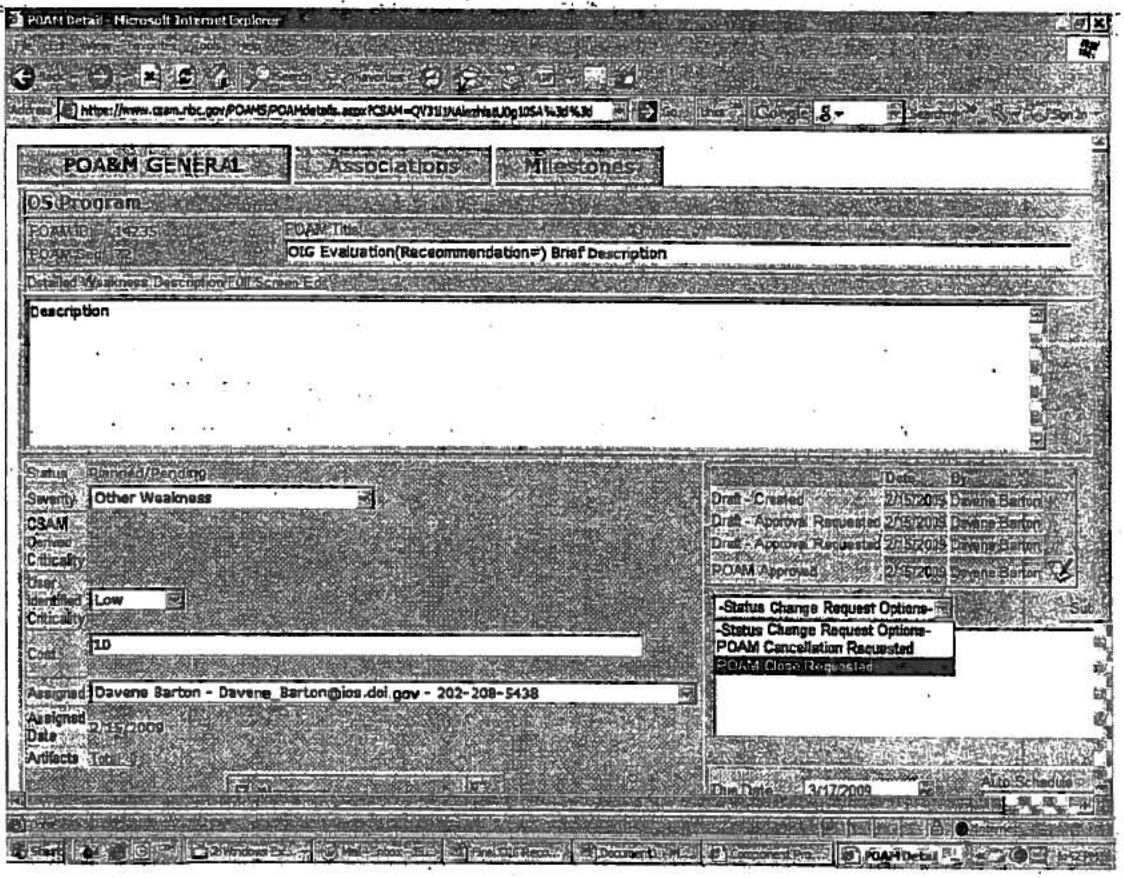
28. Select the bureau/office **Project Name** and then select the POA&M that you would like to close located on the right side of the screen under **POA&M Title.**



29. Select Edit

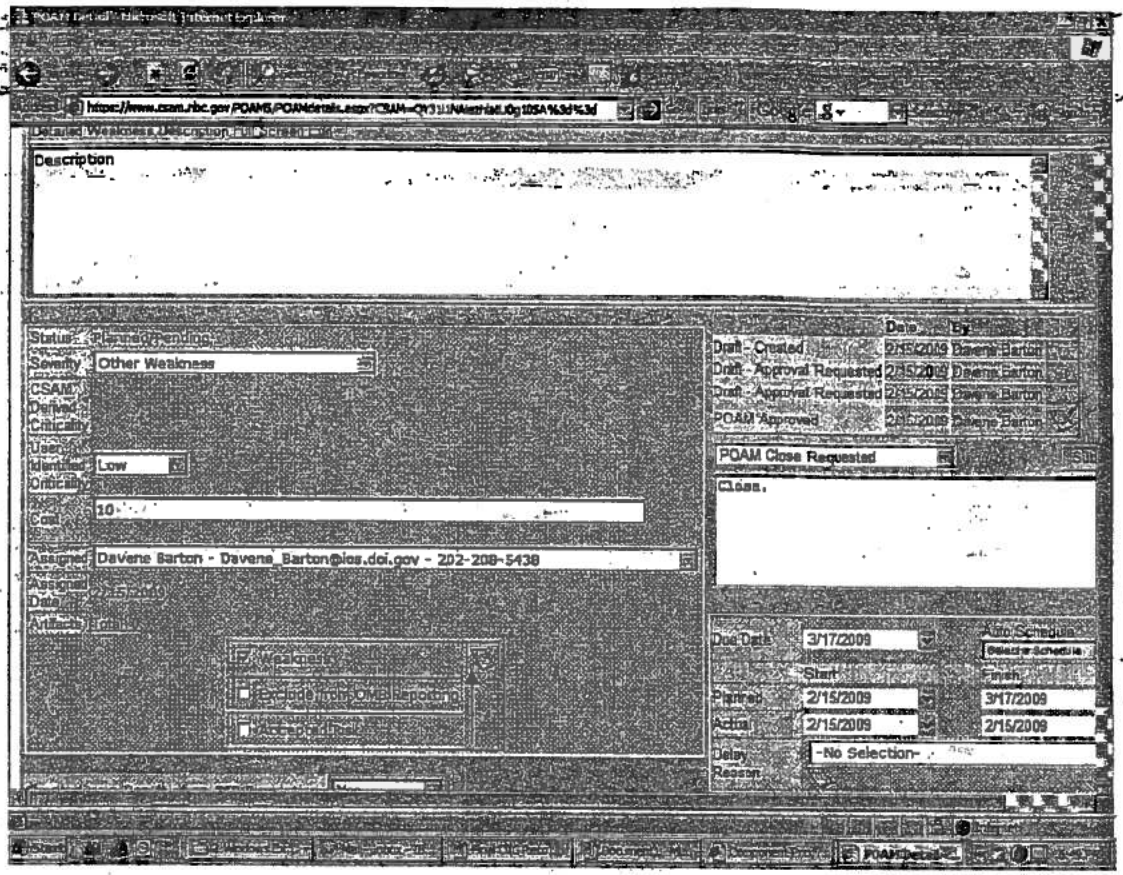


30. Select **POA&M Close Requested**, from the **Status Change Request Options**, provide comments in the text box below and then click **Submit**.

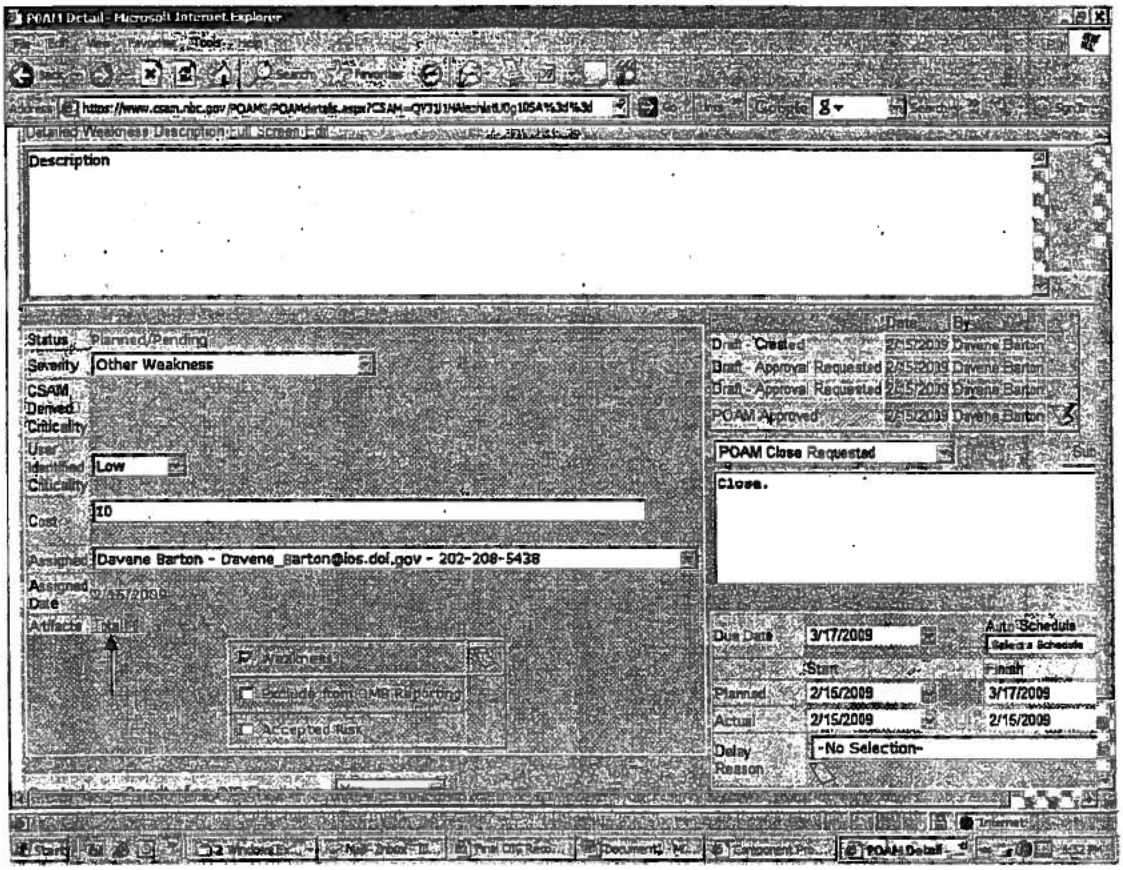


Note: After a POA&M weakness has been closed there are limited capabilities to modify them. Please ensure that newly created POA&Ms are in compliance with this standard. All POA&M weaknesses that are closed but are found to be non-compliant must be corrected or re-created with a reference to the original POA&M ID number in the POA&M Title field. The re-created (new) POA&M must reference the original POA&M ID number in the "POA&M Title" field. Additionally, the original (old) POA&M must reference the re-created POA&M ID number in the "POA&M Title" field.

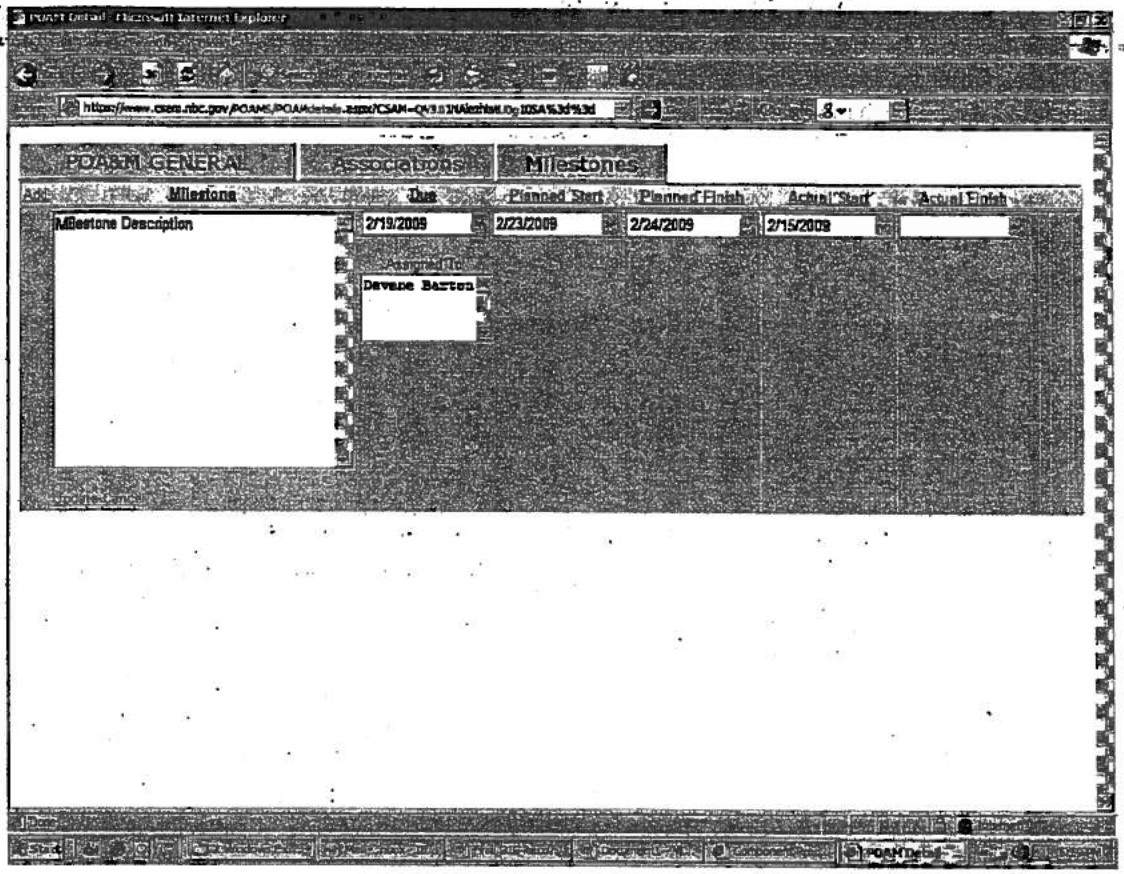
31. Select the paper icon located next to Weakness, Select **Add Comment**, enter the corrective action(s) in the comment field and select **Update**.


Description
Status
Planned/Pending
Severity
Other Weakness
CSAM Derived Criticality
User Identified Criticality
Low
Cost
10
Assigned
Davene Barton - Davene_Barton@ios.doi.gov - 202-208-5438
Assigned Date
Artifacts
Weakness
Exclude from OMB Reporting
Accepted Risk
Date
By
Draft - Created
Draft - Approval Requested
Draft - Approval Requested
POAM Approved
POAM Close Requested
Close.
Due Date
3/17/2009
Auto Schedule
Start
Finish
Planned
2/15/2009
3/17/2009
Actual
2/15/2009
2/15/2009
Delay Reason
-No Selection-

32. Click on the Total icon, to the right of Artifacts and upload artifacts such as Weakness Completion Verification Forms (WCVFs), screenshots, memorandum signature pages and other relevant evidentiary artifacts that clearly demonstrate successful resolution of the weakness.



33. Select the **Milestones** tab and then click **Add**.



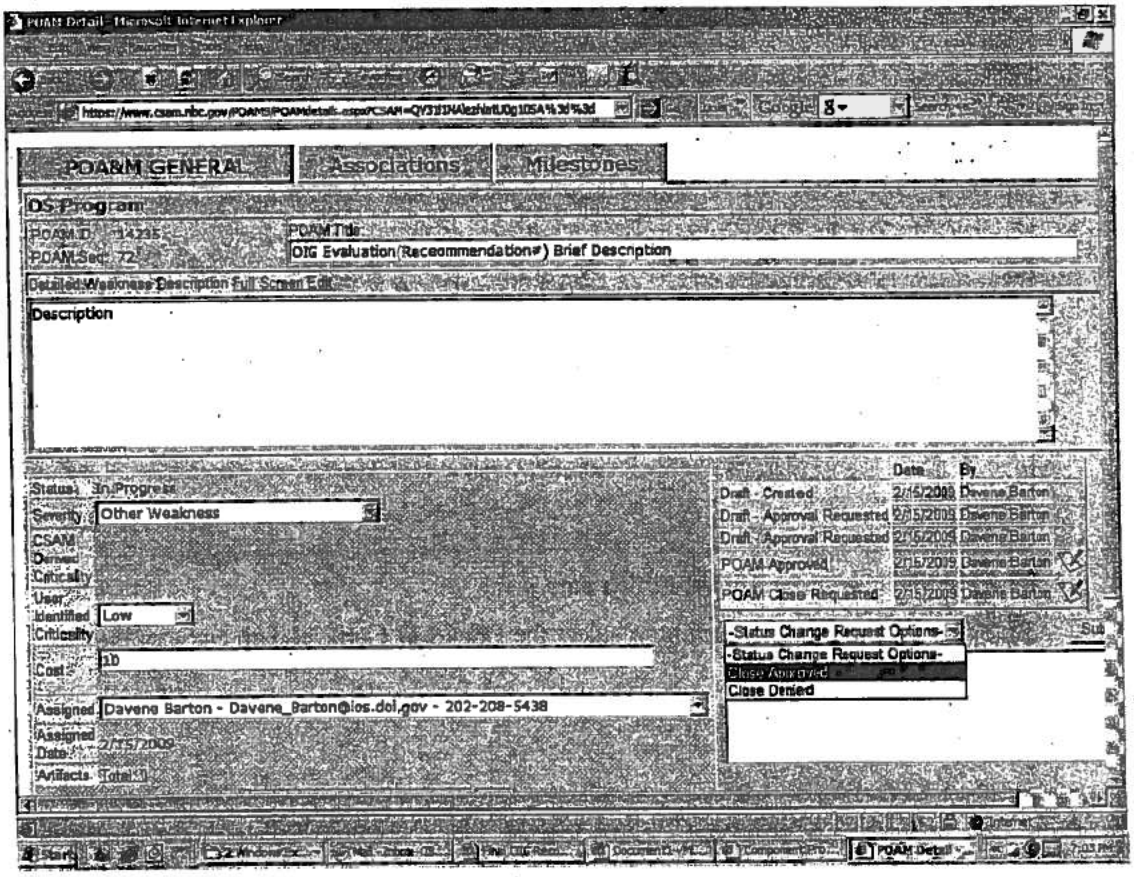
34. Enter the milestone **Actual Finish** date.

35. Select **Update** to save the entry, select the **POA&M General Tab** and exit the application.

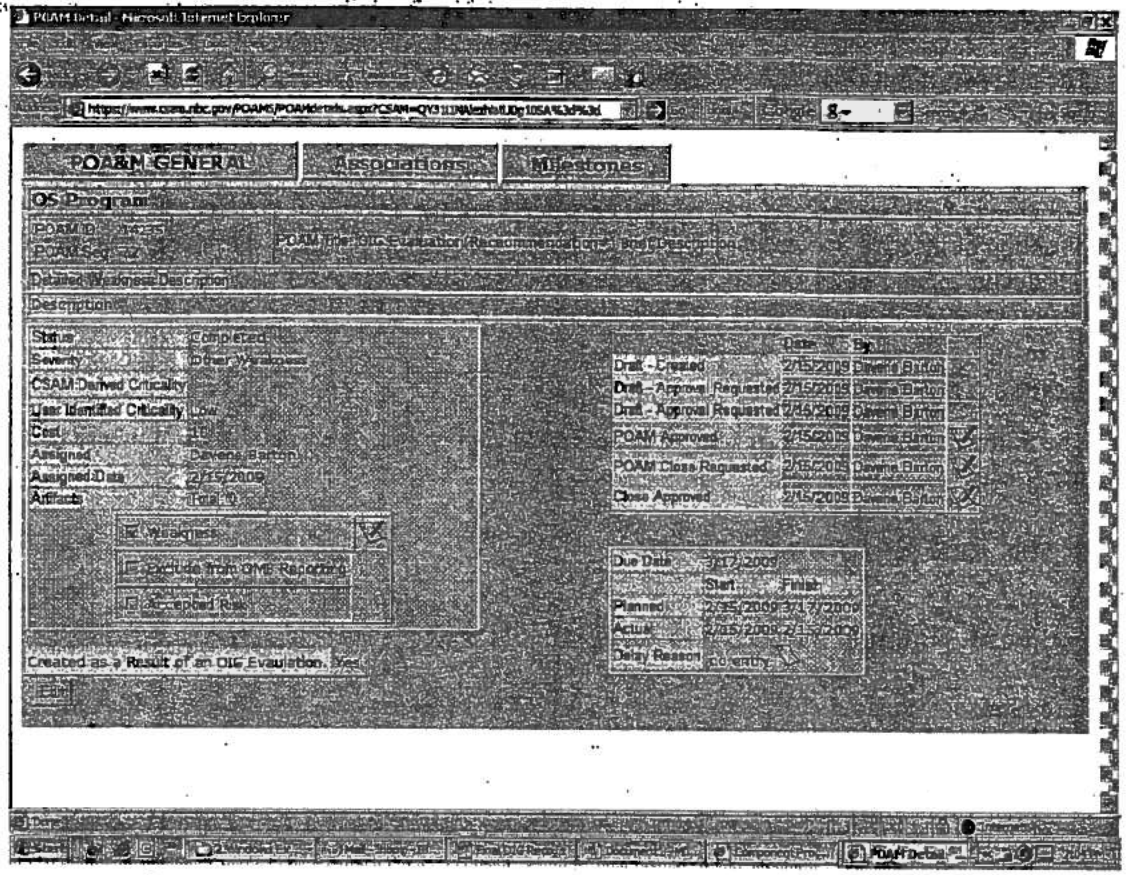
The CSD will generate a custom query report no less than quarterly on all POA&Ms that have a status of **POA&M Close Requested** and will re-evaluate the effectiveness of corrective actions. Once the CSD has determined that the weakness has been resolved to their satisfaction, the Bureau Chief Information Security Officer (BCISO) will be notified via e-mail from the CSD that the weakness has been successfully resolved.

Upon receipt of the e-mail from the CSD, return to the POA&M module in CSAM.

36. Select **Close Approved** from the **Status Change Request Options**, provide comments and then click **Submit**.



37. Enter the **Actual Finish** date and click **Save** to close the POA&M. The status will change from **In Progress, Delayed or Ongoing** to **Completed**.



Appendix G: CSAM Account Management Procedures

Purpose

The purpose of this document is to provide guidance for account management for the Cyber Security Assessment and Management (CSAM) C&A Web application henceforth referred to as "CSAM". Generally, people think of this as primarily covering the creation or changing of new user accounts (Government, contractor, regular and privileged users). However, that is just the beginning of account management. This document and the associated references also address the disabling of inactive or retired accounts and the annual recertification of accounts. Additionally, this document and its associated references also cover the processes of adding, deleting, and changing systems, components, and subcomponents to CSAM.

Scope and Applicability

The following procedures apply to all DOI CSAM application users, regardless of where they may be located.

Roles and Responsibilities

Account Manager Approving Official

The Account Manager Approving Official (AMAO) is the designated individual with authority to appoint the bureau or office Account Manager (AM). The AMAO must be the Bureau Chief Information Security Officer (BCISO), a higher official, or their duly authorized Representative as established by bureau or office BCISO in consultation with the bureau or office Chief Information Officer (CIO). The designation of all account representatives must be in writing. E-mail or signed fax is acceptable.

Account Approving Official

The Account Approving Official (AAO) is the designated individual authorized to request account creation, deletion, and modification for their respective users and/or systems. The AAO must be the system's owner, a higher official, or their duly authorized representative as established by bureau or office BCISO in consultation with the bureau or office (CIO). AAO authorization (signature, signed fax, or email is acceptable) is required on all requests prior to the requested actions being fulfilled.

Account Manager

The Account Manager (AM) is the designated individual with primary responsibilities of handling account requests and other administrative actions related to the respective bureau or office users and systems under their purview (e.g., activate, edit, and delete user accounts). Also provides ability to assign users to System Security Plans (SSP). The designation of the bureau or

office Account Manager must be in writing by the A-AO. The AM must obtain written approval from the AAO before user accounts are created, deleted or modified.

Administrator

The administrator is granted unrestricted rights to the entire system. The administrator has the ability to administer advanced functions, including updates to pick lists and templates.

Audit Log Reviewer

The Audit Log Reviewer is responsible for reviewing audit logs.

Author

The Author is the designated individual with the ability to update narratives and appendices that have been assigned. The Author can also update control-level fields (e.g. compliance description, test results, POA&Ms) for those controls that have been assigned, however, the Author does not have the ability to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping).

Authorizing Official

The Authorizing Official (AO) is responsible for conducting the quarterly review of systems under their purview prior to the submission of POA&Ms for OMB reporting; and reviewing all residual risk recommended for acceptance by the system owner, user representative, system manager, or BCISO.

Authorizing Official Designated Representative

The Authorizing Official Designated representative may be called upon to review the quarterly POA&Ms and obtain the authorizing official's signature on acceptance of any residual risks.

Bureau or Office Account Manager

The bureau or office Account Manager (AM) is the designated individual with primary responsibilities for handling account requests and other administrative actions related to the respective bureau or office users and systems under their purview (e.g., activate, edit, and delete user accounts. Also provides ability to assign users to SSPs). The designation of the bureau or office Account Manager must be in writing by the AAO. The AM must obtain written approval from the AAO before user accounts are created, deleted or modified.

Bureau or Office Chief Information Security Officer

The bureau or office Chief Information Security Officer (BCISO) is responsible for reviewing corrective actions for their respective bureau or office to ensure that each corrective action is an

effective and appropriate mitigation solution for its targeted weakness. Also, the BCISO is responsible for verifying the completion status of system security weaknesses reported in POA&Ms.

Bureau and Office Lead

The designated bureau or office representative responsible for component programs, component-level report card(s), and component FISMA reports.

Certification and Accreditation (C&A) Manager

The C&A manager shall be responsible to the bureau for ensuring adequate planning and compliance with respect to the certification and accreditation and IT security requirements, standards and guidelines issued by the Office of Management and Budget (OMB), NIST, and DOI.

Certification Agent

The certification agent is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Compliance Team

The compliance team reviews and evaluates the method of implementation and effectiveness of the bureau and office IT security programs within DOI.

Control Author

The Control Author is the designated DOI-wide representative with the ability to author security control content.

Department Lead

The designated DOI-wide representative responsible for activating, editing, and deleting bureau and office user accounts.

Information Owner

The information owner is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information System Owner

The Information System Owner (ISO) is responsible for updating the C&A package with documentation on completed POA&M items (append approved verification form.); and in coordination with the BCISO, the ISO is responsible for providing routine reviews and status reports on corrective actions to the bureau CIO and AO, no less than quarterly.
Information System Security Officer

Information System Security Officer

The ISSO is responsible for ensuring the appropriate operational security posture is maintained for an information system or program. In coordination with the ISO, the ISSO plays an active role in developing and updating the system security plan (SSP) as well as in managing and controlling changes to the system and assessing the security impact of those changes.

OCIO Reviewer

The OCIO reviewer is responsible for performing OCIO reviews for assigned SSPs and controls.

OIG Reviewer

The OIG reviewers are granted read-only access to all program and system-level POA&Ms.

POA&M Coordinator

The POA&M coordinator is responsible for entering updated POA&M and or POA&M data from the System Owners or their designees and consolidating POA&Ms for quarterly submission to the Cyber Security Division (CSD).

Primary Author

The Primary Author is the designated individual with the ability to make updates to all fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping). The Primary Author also has the ability to assign control-level edit access and appendix and narrative update access to him/herself and other users (e.g. Authors, Validators).

Program Manager

The Program Manager is responsible for updating the C&A package with documentation on completed POA&M items (append approved verification form.); and in coordination with the BCISO, the ISO is responsible for providing routine reviews and status reports on corrective actions to the bureau CIO and AO, no less than quarterly.

Senior Agency Information Security Officer

The Senior Agency information Security Officer or Department Chief Information Security Officer is the DOI official responsible for carrying out the DOI Chief Information Officer IT security and compliance responsibilities under FISMA.

SME - CM

The department has the ability to update the CM report card indicator for each bureau or office.

SME – Incident Response

The department has the ability to update the Incident Response indicators in the report card for each bureau or office.

SME – Training (Department)

The department has the ability to view and update Awareness and IT Professional Training numbers for each bureau or office.

SME – Training (Bureau or Office)

The bureau or office has the ability to update reported training numbers for Awareness and IT Professional Training.

SSP Reviewer

The SSP reviewer is granted read-only view to all SSPs in each assigned bureau or office.

User Representative

User representatives are responsible for the identification of mission/operational requirements and for complying with the security requirements and security controls described in the system security plan. User representatives are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the life cycle of the information system.

Validator

The Validator is the designated individual with the ability to update only test results, but can be given privilege to update cost, compliance description, and POA&Ms. The Validator can also update narratives and appendices if assigned. The Validator will not be able to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping).

Management Procedures

Bureaus and offices shall comply with the NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, identification and authentication controls identified in the *DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008.
Before an account can be set up in CSAM a User Account Profile worksheet and a System Profile worksheet must be completed. The worksheet format/layout tries to emulate what appears within CSAM.

In the User Account Profile worksheet and the System Profile worksheet DOI has used the comment feature to provide a wealth of additional detailed information. Cells with comments are indicated by a small red triangle in the upper right corner of that cell. Comments are usually immediately available as the document is completed online. Comments can usually be viewed simply by placing the cursor on that particular cell.

AAOs are responsible for all user accounts and systems under their jurisdiction through all phases from creation, annual recertification, and inactivity to retirement. The AAOs (or their duly authorized Representative) must notify their respective AM whenever anyone leaves, transfers, or no longer needs access to CSAM in order to have their account disabled **within two business days** of the event occurring.

Hard copy or fax of input, signatures, etc. is acceptable however not preferred. The preferred media is e-mail; this enables a more efficient method of maintaining a trail of evidence rather than that of paper. Acknowledgements must be explicit. There can be no doubt about who is acknowledging and what they are acknowledging. Please remember that the AM must maintain a trail of evidence for all actions taken. This is especially needed when unusual activities are requested. DOI personnel need to document the authorization as well as the justification for those actions.

User Account

The User Account procedures are provided within the User Account Profile worksheet. CSAM has a means by which the user inputs their personal profile information directly, however, the process to authorize that account, role, and permissions as well as the user's acknowledgement of the DOI Rules of Behavior (ROB) must still be handled manually. A basic CSAM integration evolution within an enterprise involves the establishment of new user accounts.
The worksheet provides procedures to effectively support the profiling of new users so that appropriately profiled new user accounts can be established efficiently and accurately.

The worksheet is divided into three parts:

Part A – User Information. This section identifies general items required such as the user's name, bureau or office name, whether the user is a Government Employee or Contractor and the name of the authorizer of the account (e.g., System Owner) and systems to access.

Part B – Special Access. This section identifies special access privileges for component (also known as bureau or office) users and department/headquarter users. Special access privileges will be granted to bureau/office and department leads only.

Component special access privileges provide:

* Access to bureau or office Report Card
* Access to bureau or office FISMA Reports
* Ability to give existing users access to component SSPs

Department/Headquarter special access privileges provide:

* Access to Department Programs
* Access to Department Report Card
* Access to Department FISMA Reports
* Ability to give existing users access to SSPs
* Ability to add SSPs
* Ability to update Report Card manual columns
* Ability to run Department POAM Report

Part C - Edit Privileges. This section identifies actions that need to be taken once the information and authorization of Parts A & B have been completed by the user or AAO and inputted by the AM. For example, the name of the system(s) the user should have access to, whether or not the system should be provided during the training phase of the migration process, if the user is to have access to this system for production purposes after migration is complete, if the user should be a/the Primary Author for the System's SSP. [This allows the user to add other users to the SSP and assign them tasks]

The information for Parts A & B must be completed and submitted before the AM can perform the requested action(s). Any and all incomplete forms will be returned to the submitter.
The user has limited ability to see their account profile information. Any changes to their account profile information need to be made through the AM. After establishing the CSAM account, the user then needs to be provided access to the systems requested. This can be accomplished by the AM or by a bureau or office lead or Primary Author associated with that system. We prefer that this be accomplished at the bureau or office level so that they are fully engaged with managing their accounts, etc. For a new Primary Author or Author, this is accomplished by going into each system and adding the new user under the "Assign Roles" user access list for that system. A bureau or office lead automatically has access to all systems under that bureau or office. The bureau or office lead should update the "Assign Roles" user access list for each system for documentation purposes.

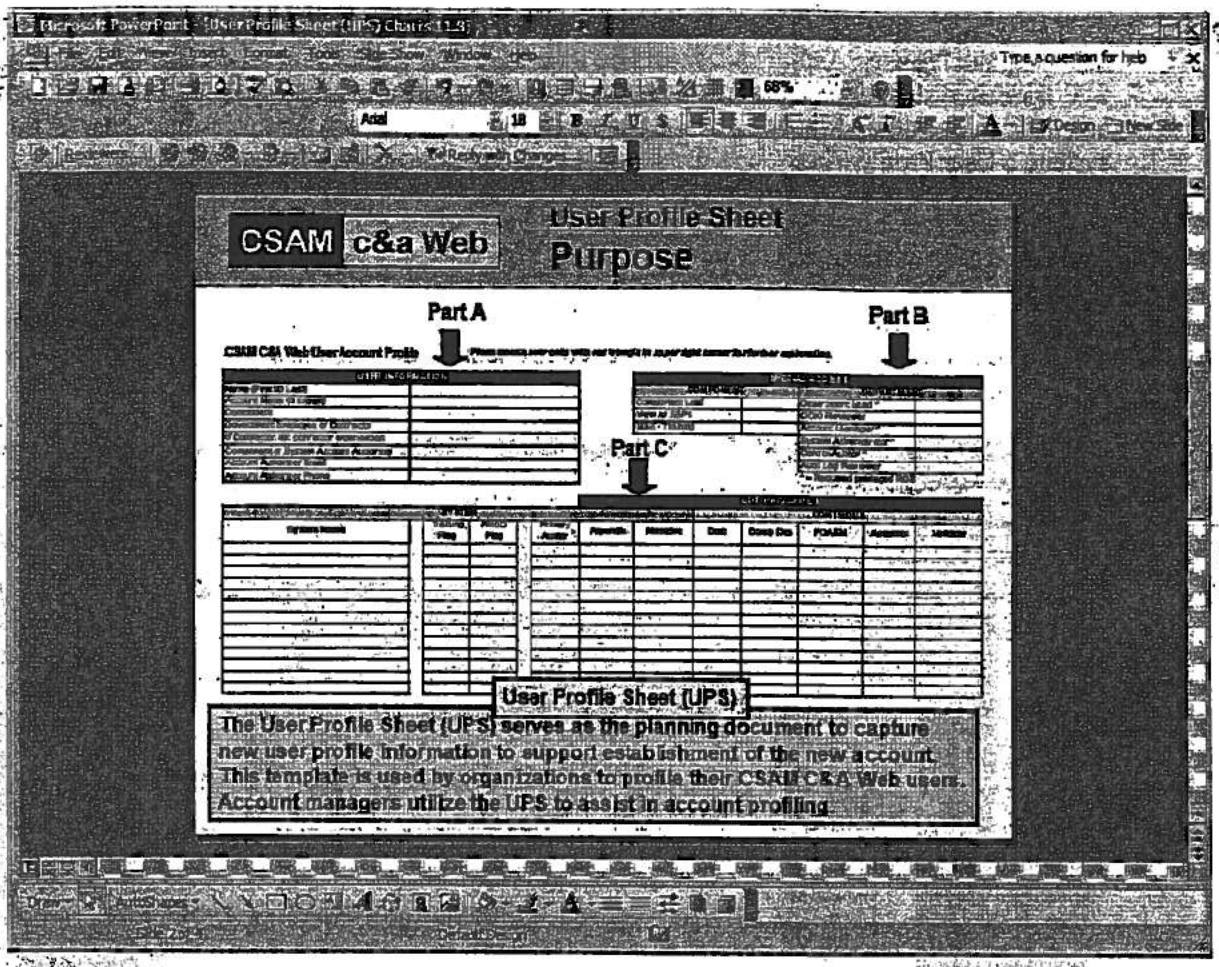


Figure 3 User Profile Sheet

The User Profile Sheet is embedded in the following logo. If you double click on the logo, the form will open. It can be saved to a separate file for future use.

Final User Profile Sheet 013008.xls

Systems, Components & Subcomponents

The System Profile worksheet identifies the information needed when a new system is added to CSAM. This also serves to identify what system(s) a new account needs access to although the System Owner should provide this access. This worksheet has two parts:

Part A- Identifies the basic information needed to establish a new system or identify which system(s) a new account needs access to. For a new system, pay special attention to the comments in the Operational Status field.

Part B - Once the system has been established by the actions associated with Part A, at least one user with the Primary Author role should be identified who will be responsible for updating the SSP for this system. The Primary Author will be able to manage user access to this system and add and remove other Authors, and Validators. If they do not already have a user account on the system, a User Profile Sheet must also be submitted by the user's account authorizer.

Incomplete forms may delay the processing of your request(s). Please choose your system names and abbreviations carefully.

Typically this form is used for creating new systems. However, the comments also provide information on retiring systems, adding components, subcomponents and other valuable information.

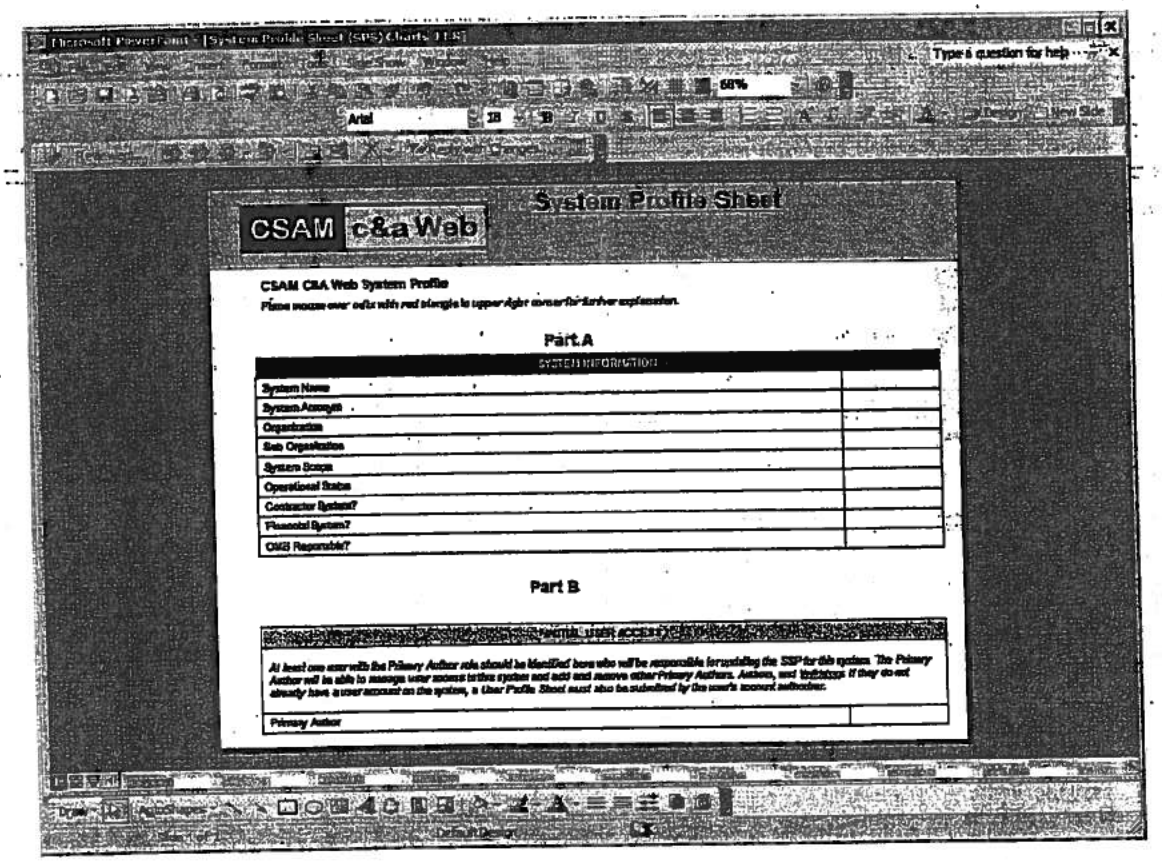


Figure 4 System Profile Sheet

The System Profile Sheet is embedded in the following logo. If you double click on the logo,the form will open. It can be saved to a separate file for future use.

Final System Profile 013008.xls

Recertification

Recertification of user accounts will be handled directly in CSAM whenever possible, concluding with a report generated from the application that will be sent out for review and signature by the bureau or office AAO (CISO) or CISO designated Representative.

User Account Auditing Procedures

All accounts are automatically locked after 90 days of inactivity. Accounts can also be locked manually by the AM, and a notation can be recorded in a comment field to indicate why the account was locked.

A list of locked accounts is forwarded to the OCIO Client Representative for determination, in conjunction with the bureau or office AO or AM, if the account is still required. If the account is no longer needed, the account status is changed to "Inactive" and the account comments are updated. User capabilities are removed from accounts when they are retired or inactive for more than 90 days and a notation is entered in the account profile. An entry is then made to record when a bureau or office account was audited and the number of accounts locked. OCIO management can then monitor that this weekly audit activity is occurring.

Accounts with user administration capabilities are reviewed on a quarterly basis to determine if user administrator functions are still required.

Definitions

1. **Account**: A logical representation of a user in a system, which allows a user to gain access to the system. Examples of user accounts include the following: Microsoft Active Directory Service accounts, UNIX accounts on individual servers, Oracle database accounts, application accounts, and accounts on devices such as LAN infrastructure equipment.

2. **Account Creation**: The process of creating a new user account.

3. **Account Disablement**: The process of disabling a user account. Disabling a user account does not completely remove the account. Rather, it prevents the user account from being used to gain access to the system.

4. **Account Manager**: A role in the CSAM system that provides ability to activate, edit, and delete user accounts. Also provides ability to assign users to SSPs.

5. **Account Modification**: The process of moving a user from one program office or bureau to another. In such circumstances, an account is moved from one operating system level user group to another.

6. **Account Retirement**: The process of disabling a user account for a user who has departed an organization.

7. **Author**: A role in the CSAM system that will not be able to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping), but can update narratives and appendices that have been assigned. The Author can also update control-level fields (e.g. compliance description, test results, POA&Ms) for those controls that have been assigned.

8. **Control Author:** a role in the CSAM system that is the designated DOI-wide Representative responsible for defining DOI specific controls for developing C&A packages.

9. **Department Lead:** The designated DOI-wide Representative responsible for activating, editing, and deleting bureau and office Account Manager user accounts.

10. **Primary Author**: A role in the CSAM system that has the ability to make updates to all fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping),

can assign control-level edit access and appendix and narrative update access to self and other users (e.g. Authors, Validators).

11. **Transfer Account**: The process of transferring a user account from one office to another office, within the same component.

12. **Validator**: A role in the CSMA system that will not be able to update most fields of an SSP (e.g. system characteristics, boundary definition, requirements scoping). Typically individuals in this role update only test results, but can be given privilege to update cost, compliance description, and POA&Ms. The Validator can also update narratives and appendices if assigned.

Appendix I: CSAM Rules of Behavior

Purpose

The purpose of this document is to explain the Rules of Behavior and requirements to all DOI employees who use CSAM, as specified by OMB Circular A-130, the *DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008, and other related policies. DOI IT resources are the property of the Federal Government and must be protected. Users' access to computing resources indicates a level of trust given to the employees by management and ultimately by DOI. Users must be aware of and acknowledge their actions and their responsibilities when using CSAM in accordance with these Rules of Behavior.

Scope

These Rules of Behavior apply to all employees and contractors who use CSAM. All DOI employees who access CSAM that requires a user ID must be aware of their responsibilities and comply with these Rules of Behavior.

Penalties for Non-Compliance

These Rules of Behavior are founded on the principles described in the DOI published security policies and other regulatory documents such as the Code of Ethics for Government Employees, OPM regulations, OMB regulations, and Standards of Conduct for Federal Employees. Therefore, these rules carry the same responsibility for compliance as the official documents cited above. DOI will apply penalties for noncompliance in a uniform and consistent fashion regardless of race, sex, color, national origin, disability, religion, marital status, grade level, or bargaining unit status of the personnel involved. Account Managers must exercise sound and reasonable judgment in enforcing these Rules of Behavior. Penalties will be assessed in a timely manner. DOI will enforce the use of penalties against any user who willfully violates any DOI or Federal system security policy, including:

- Official, written reprimands,
- Suspension of system privileges,
- Temporary suspension from duty,
- Removal from current position,
- Termination of employment; and
- Possible criminal prosecution.

General Requirements

The Rules of Behavior presented in this document highlight requirements from several laws, policies, and best practices. These Rules of Behavior establish expected and acceptable computing behaviors. Because written guidance cannot cover every contingency, users are also asked to use sound judgment and the highest ethical standards in their decision making.

Access

Users shall access and use only information for which they have official authorization. The following guidelines also apply:

- Follow established procedures for accessing information, including use of user identification, user authentication, passwords, and other physical and logical safeguards,
- Follow established channels for requesting and disseminating information,
- Access only those files, directories, and applications for which access authorization by the system administrator has been granted,
- Use government equipment only for approved purposes,
- Do not give information to other employees or outside individuals who do not have access authority,
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties; and
- Do not browse files (look to see what you can access).

Accountability

Users are accountable for actions related to information resources entrusted to them.

- Behave in an ethically, technically proficient, informed, and trustworthy manner when using systems,
- Be alert to threats and vulnerabilities such as malicious programs and viruses,
- Prevent others from using your accounts by using procedures such as the following:
  - Log out or lock the screen when leaving the vicinity of your terminal or PC,
  - Set a password on automatic screen savers,
  - Help remedy security breaches, regardless of who is at fault; and
  - Immediately notify the system administrator whenever there is a change in your role, assignment, or employment status and/or when access to the system is no longer required.
- Participate in IT security training and awareness programs,
- Do not install or use unauthorized software on DOI equipment,
- Comply with all software licensing agreements; do not violate Federal copyright laws,
- Practice good citizenship when accessing external systems by complying with that system's rules of behavior; and
- Read and understand banner pages and end user licensing agreements.

Integrity

Users must protect the integrity and quality of information.

- Review quality of information as it is collected, generated, and used to ensure that it is accurate, complete, and up to date,
- Take appropriate training before using CSAM to learn how to correctly enter and change data,
- Protect information against viruses and similar malicious code by:
  - Using virus detection and correction software,
  - Avoiding unofficial software, such as shareware and public domain software; and
  - Discontinuing use of a system at the first sign of virus infection,
- Never enter unauthorized, inaccurate, or false information into a system.

Availability

Computer systems and media must be protected from environmental factors such as fire, water, heat, and food spills. They must also be protected from theft, unauthorized alteration, and careless handling.

- Use physical and logical protective measures to prevent loss of availability of information and systems, such as:
  - Ensuring that there are backups of information for which you are responsible,
  - Protecting systems and media where information is stored,
  - Storing media in protective jackets,
  - Keeping media away from devices that produce magnetic fields (such as phones, radios, and magnets),
- Follow contingency plans; and
- Ensure that more than one individual knows where to find important information and has access rights.

Passwords and User IDs

Users are responsible and accountable for any actions taken under their user ID.

- Protect passwords from access by other individuals,
- Never give a password to another person (including your supervisor or a computer support person); and
- Do not ask anyone for their password.
- Construct effective passwords in accordance with the *DOI IT Security Policy Handbook*, Version 3.1, March 18, 2008.

Privileged Users

Privileged users are those with one or more of the following functions:

- System administrators,
- Departmental CSAM Account Manager,
- System engineers (those with control of the operating system),

- Network administrators,
- Database administrators; and
- Those who control user passwords and access levels.

Privileged users must make an effort to notice the threats to and vulnerabilities of CSAM, call these to the attention of management, and work to develop effective countermeasures.

Privileged users will:

- Respond to security alerts and requests by the Department CISO,
- Protect the supervisor or root-level password at the highest level demanded by the sensitivity of the system,
- Use special access privileges only when they are needed to carry out a specific system function,
- Use a non-privileged account whenever possible,
- Never use special privileges for personal business, gain, or entertainment,
- Use precautionary procedures to protect a privileged account from fraudulent use,
- Establish security measures to ensure integrity, confidentiality, and availability of information contained on the systems,
- Watch for signs of hacker activity or other attempts at unauthorized access,
- Assist with recovery activities and take appropriate action to reduce damage from security violations,
- Alert the appropriate personnel when a system goes down or experiences problems, and
- Ensure that systems and data are properly backed up and that the configuration is adequately documented for recovery purposes.

I acknowledge receipt of the Rules of Behavior, understand my responsibilities, and will comply with the CSAM Rules of Behavior.

_____ _____

Signature Date

Note: Statement of acknowledgement must be provided to your bureau or office Account Manager.

United States
Department of the Interior

Reviewed
8/3/2011

Role-Based Security Training (RBST) Standard v2.6.0

March 11, 2011

Document Change History

Version Number	Release Date	Summary of Changes	Section Number/ Paragraph Number	Changes Made By
1.0	01/13/2007	Bureau Comments Incorporated	Various	Mikki Smith
1.2	10/05/2007	ITST Staffing of Updated Comments	Various	ITST Training Subcommittee
1.3	01/30/2008	Final Draft for CIO Review/Promulgation.	Various	CSD
2.0	7/17/2009	•Provided additional detail per NIST SP 800-16 Rev 1 draft •Changed the security training groupings to be consistent with OPM 5 CFR Part 930 •Allowed the maintenance of DOI approved information security certifications to satisfy RBST requirements •Added an enforcement clause for the completion of mandated training •Added Appendices C – E, which should be reviewed and updated each fiscal year	Various	Lance Kelson
2.1	8/17/2009	Incorporated input from IT SEAT WG and CSD	Various	IT SEAT WG
2.2	8/25/2009	Incorporated input from ITST	1.4	ITST
2.3	9/22/2009	Replaced arbitrary minimum required hours of training annually for each security training group with minimum number of Information Security Training Focus Areas	2.1	Larry Ruffin, Chris Rutherford
2.4	10/2/2009	Final Draft for CIO Review/Promulgation	2.1	Lance Kelson
2.5	11/3/2009	Incorporated input from PAM •Define DOI personnel as employees and contractors •Reiterate minimum requirements •Removed language covering financial responsibility for RBST	1.2 App D 2.3	Lance Kelson
2.5.1	3/11/2010	Incorporated the 'Approved' list of Classes/Focus Areas within App D	App D	FWS: Tyler Marriott, Lan Nguyen BLM: D'Andrea S Spann
2.6.0	3/4/2011	•Removed references to Extra Transcript Items and Certification and Accreditation. •Changed RBST artifact retention requirement to 12 months	2.1	Lance Kelson

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 BACKGROUND 1
1.2 PURPOSE 1
1.3 SCOPE 2
1.4 AUTHORITY 2
1.5 DEFINITIONS 4
1.6 STRUCTURE 4

2 DOI ROLE-BASED SECURITY TRAINING STANDARD 5

2.1 DOI INFORMATION SECURITY TRAINING GROUPS 5
2.2 ASSIGNING PERSONNEL TO INFORMATION SECURITY TRAINING GROUPS 9
2.3 TRAINING TO CONTRACTORS 10
2.4 TRAINING CONTENT 10

3 DOI ROLE-BASED SECURITY TRAINING, TRACKING AND COMPLIANCE REPORTING 11

3.1 MANAGEMENT AND TRACKING 11
3.2 COMPLIANCE REPORTING 11

APPENDIX A – ACRONYMS 12

APPENDIX B – REFERENCES 14

APPENDIX C - LISTING OF DOI RECOGNIZED INFORMATION SECURITY PROFESSIONAL CREDENTIALS 15

1 INTRODUCTION

1.1 BACKGROUND

Information Security is a top Department of the Interior (DOI) priority. A strong Departmental IT Security Program (ITSP) cannot be sustained without an investment in training. To be most effective, training must focus on key information security issues such as security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure information resources. Failure to adequately address information security training places the Department's information and information systems at greater than acceptable risk.

Accordingly, the Department has established a comprehensive, measurable, and cost-effective Role-Based Security Training Standard that will enable Bureaus and Offices to strengthen their existing Information Security Training Programs, and thus strengthen the Department's overall ITSP. A robust and Department-wide training program is paramount to ensuring that personnel understand their information security responsibilities, Departmental policies, and how to properly protect information resources entrusted to them.

All levels of personnel have roles to play in the success of the ITSP. However, Bureau/Office Heads, Human Resources Managers, Chief Information Officers (CIO's), Program Managers, Bureau Training Managers, Contracting Officers, and Bureau/Office Chief Information Security Officers (CISO's) have key responsibilities to ensure that an effective program is implemented throughout their Bureaus or Offices.

1.2 PURPOSE

The purpose of the *DOI Role-Based Security Training (RBST) Standard* is to provide Bureaus and Offices with requirements and guidance to enhance their ability to provide appropriate role-based security training for DOI personnel, which includes employees and contractors. The Standard focuses on requirements that are associated with job functions, or roles and responsibilities specific to individuals having significant information security responsibilities. It provides a planning framework to identify training requirements and needs throughout the workforce and ensures that applicable personnel receive appropriate training. This guide provides Bureau/Office Human Resources Managers, contract management staff, supervisors and training administrators with guidance to identify personnel who are required to receive role-based security training, categorize those personnel into appropriate training groups, and report on training compliance for those groups.

1.3 SCOPE

This Standard covers the RBST requirements for all DOI employees and contractors[1] who have elevated privileges or significant information security responsibilities for DOI information systems. Specifically, anyone that manages, acquires, designs and develops, implements and operates, and/or reviews and evaluates any of the NIST SP800-53[2] security controls has significant information security responsibilities. Such training requirements extend beyond those individuals with direct information system or information security responsibilities. They also encompass those individuals with mission or non-IT program responsibilities, where those responsibilities are supported through the use of information systems such as system owners and Authorizing Officials/Designated Accreditation Authorities.

This standard describes the federal requirements for RBST; identifies key stakeholders responsible for compliance; establishes the minimum DOI requirements for role-based security training based on roles, responsibilities and functions; and defines DOI RBST tracking and reporting criteria. RBST requirements for persons with significant information security responsibilities, including Information Security Basics, are in addition to mandatory annual Federal Information System Security Awareness (FISSA) training.

1.4 AUTHORITY

Federal requirements addressing the role-based security training of DOI personnel are summarized below. These requirements provide the foundational authority for this Standard. For each requirements document identified, a specific citation addressing information security training requirements has been excerpted to identify key responsibilities and training obligations.

- **Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources***

  "Training. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system."

  "Specialized Training[3]. ....ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application)."

---

[1] See Section 2.3 Training to Contractors

[2] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

[3] The OMB Circular employs the term "Specialized Training" in lieu of "Role-based Security Training" when referring to required supplemental information security training.

- **Federal Information Security Management Act (FISMA), Title III – Information Security**

  "...security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of— (A) information security risks associated with their activities; (B) and their responsibilities in complying with agency policies and procedures designed to reduce these risks."

  FISMA requires that the head of each agency *"delegate to the agency Chief Information Officer...the authority to ensure compliance with the requirements imposed on the agency...,including— training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities..."*

- **Office of Personnel Management (OPM), 5 CFR Part 930,** ***Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems:***

  "Each Executive Agency must develop a plan for Federal information systems security awareness and training and

  > *(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance available on the NIST Web site, http://csrc.nist.gov/publications/nistpubs/"*

- **National Institute of Standards and Technology (NIST) Special Publication 800-16, Revision 1 (Draft)** ***Information Security Training Requirements: A Role- and Performance-Based Model***[4]

  "FISMA requires agencies to identify and train those personnel with significant responsibilities for information security. These personnel - whether executives, information security program staff members, or system/network administrators - are in positions that are responsible for the security of the organization's information and information systems. Because of their positions, they can have the greatest positive or negative impact on the confidentiality, integrity, and/or availability of agency information and information systems. Specialized role-based information security training is necessary to help ensure that these "keys to security" clearly understand that information security is an integral part of their job; what the organization expects of them; how to implement and maintain information security controls; mitigate risk to information and information systems; monitor the security condition of the security program, system, application, or information for which they are responsible; and/or what to do when security breaches are discovered. These personnel must:

  - *Attend role-based training identified/approved by their management,*
  - *Advise their management of additional training that can help them better secure information and information systems for which they are responsible, and*

[4] This citation is excerpted from Section 1.5.6 "Personnel with Significant Responsibilities for Information Security". Roles and responsibilities for personnel with significant responsibilities for information security appearing in the final version of SP 800-16, Rev 1 will be the updated corresponding requirement in this standard.

- *Apply what is learned during training."*

- **OPM 5 CFR, Part 410.701(a)(b) - Training; Reporting Requirements**

  "(a) Each agency shall maintain records of training plans, expenditures, and activities in such form and manner as necessary to submit the recorded data to the Office of Personnel Management (OPM) through the OPM Governmentwide Electronic Data Collection System.

  (b) Beginning December 31, 2006, each agency shall report the training data for its employees' training and development at such times and in such form as required for the OPM Governmentwide Electronic Data Collection System, which is explained in the Guide to Personnel Recordkeeping and the Guide to Human Resources Reporting. "

- **Departmental Manual Part 370, Chapter 752 *"Discipline and Adverse Actions", Table of Offenses and Penalties, General Misconduct***

  "Failure or delay in carrying out instructions; failure or carelessness in performing assigned work; failure to take/complete officially-directed training. "

  - *Penalty for First Offense: Written Reprimand to 14-day suspension*
  - *Penalty for Second Offense: 14- to 30- day suspension*
  - *Penalty for Third Offense: 30- day suspension to removal*

1.5 DEFINITIONS

For purposes of this Standard, DOI defines "significant information security responsibility" as any individual whose job role or function includes any of the following:

- Elevated or advanced rights, beyond a general user, to DOI IT systems for information system support and administration purposes;
- Bureau/Office and Departmental officials providing information security program management, oversight, policy, compliance, implementation or information security support responsibilities;
- IT managers and executives providing IT program management, oversight, policy, compliance or implementation responsibilities; and
- Other staff that have functions that impact the implementation, maintenance, or evaluation of cyber security above their own user level.

1.6 STRUCTURE

This standard is organized into three major sections:

- Section 1: **Introduction** – introduces the standard and federal requirements
- Section 2: **DOI Role-Based Security Training Standard** – details departmental mandates and standards for role-based security training; and
- Section 3: **DOI Role-Based Security Training Tracking and Compliance Reporting** - describes the required reporting and tracking processes.

2 DOI ROLE-BASED SECURITY TRAINING STANDARD

2.1 DOI INFORMATION SECURITY TRAINING GROUPS

An analysis of the job functions within DOI Bureaus and Offices, DOI's definition of "significant information security responsibility" in section 1.5 of this Standard, OPM mandates, and the recommendations from NIST has led to the establishment of four role-based training group designations. These groups should be considered a training program starting point. Bureaus and Offices may identify and require that additional roles and functions require RBST. Such determinations should be based on assessed risk or impact and/or operational need. Any additional Bureau- or Office-specific training requirements should be identified in Bureau or Office security documentation (policy or guidance documents) or in the appropriate System Security Plan (SSP).

Each group shall have minimum RBST Requirements. In General:

1. Bureau/Office Heads shall ensure that all personnel identified having significant information security responsibilities receive role-based security training annually.
2. Bureau/Office Training Managers, HR personnel, supervisors, and Bureau/Office CISOs are responsible for collaborating to develop information security training plans for personnel that include the mandated training requirements outlined in this standard. Supervisors, in consultation with the employee, are in the best position to determine individual employee's training needs, consistent with the employee's Performance Appraisal Plan and Individual Development Plan.
3. It is the responsibility of the employee and supervisor, contractor and contract management staff, and the Bureau/Office CISO to ensure that the employee/contractor has sufficient RBST to adequately fulfill the information security responsibilities of his/her assigned role.
4. Bureau/Office Heads will ensure that training plans are established and implemented in accordance with NIST Special Publication 800-16. Emphasis should be placed, to the extent possible, in providing training specifically based on current job roles rather than general Information Security topics.
5. Bureaus and Offices may provide additional, technology specific education and training to employees and contractors via online training, classroom instruction, seminars, or security forums. Since DOI LEARN is the system of record for training for DOI, such training will be recorded in the employee/contractor's DOI LEARN transcript but may not be applicable to RBST requirements unless approved by the BCISO or his/her designate. It is at the discretion of the Bureau or Office to determine the most cost-effective sources for training to meet the training needs of personnel filling supporting information system roles. To the extent practical, Bureaus and Offices shall utilize the Department's on-line centralized solution, DOI LEARN, for any RBST provided to employees/contractors with significant information security roles and responsibilities to enable consistent and effective tracking.

6. Employee RBST completed outside of DOI LEARN shall include creation of an SF 182[5] entry in DOI LEARN, which must be approved by supervisors. Bureaus and Offices will utilize the SF 182 in DOI LEARN to track and facilitate reporting of RBST costs outside of DOI LEARN for employees.
7. Evidence (e.g. certificates of completion, or professional credential certificates and associated continuing education transcripts) of employee/contractor RBST completed outside of DOI LEARN shall be retained for twelve months after completion of the activity.
8. Bureaus and Offices must coordinate with their appointed DOI LEARN Managers and Data Stewards to ensure that required courses have been assigned to applicable employee/contractors' course lists within DOI LEARN. To determine the DOI LEARN point of contact for each Bureau or Office, visit: http://www.doi.gov/hrm/DOILearn.html .
9. In cases where an employee/contractor has multiple roles, and multiple training groups may apply, the training group assignment should be designated based on the training requirements of the employee/contractor's most rigorous job role and function. For example, a senior management official with Information Owners responsibilities who also serves as an Information System Security Officers (ISSO) should be assigned to the Information Security Personnel group, as opposed to the Executive and Senior Management group, based on the more rigorous training requirements of the former.
10. Acquisition and maintenance of a recognized information security professional credential may be substituted for the RBST group requirements described in the sections below. Evidence of these activities related to information security professional credentials must be presented to the BCISO or his/her designate and retained by the contractor/employee. See Appendix C for a listing of DOI recognized information security professional credentials for the current fiscal year.
11. To facilitate tracking of RBST completions, Bureaus and Offices have the option of requiring RBST designated participants to complete a DOI-wide RBST self-certifying course available in DOI LEARN upon completion of their annual RBST requirements to certify they understood and completed their fiscal year RBST requirements. Assertions that RBST requirements have been met by self-certification must be validated by supervisors and are subject to audit by Human Resources, OCIO, and the Office of the Inspector General. Supervisors and managers are responsible for validating that direct reports assigned RBST have completed their annual RBST requirements.

[5] OPM Memorandum dated July 2, 2007, New Standard Form (SF) 182, Authorization, Agreement and Certification of Training Form

- **Group 1 - Executive and Senior Management**
  - Consists of DOI Senior Executive Level and other senior management personnel whose job functions may include IT management activities that typically extend and apply to an entire organization or major components of an organization. This includes, but is not necessarily limited to, strategic planning, capital planning and investment control, workforce planning, policy and standards development, resource management, knowledge management, architecture and infrastructure planning and management, auditing, and information security management.
  - Group membership includes:
    - Bureau, Regional, and Office IT Division Heads
    - Chief Information Officers (CIOs)
    - Deputy Chief Information Officers (DCIOs)
    - Authorizing Officials (AOs) or Designated Approving/Accrediting Authorities (DAAs)
    - User Representatives
    - Information System Owners
    - Information Owners
  - Information Security Training Focus Areas[7] – training should include at least 1 of the following:
    - Information Security Basics
    - Policy Level Security Planning and Management
    - Emergency Management and Disaster Recovery
    - Strategic Security Planning or Implementation
    - Risk Management Framework
- **Group 2 - Program and Functional Management –**
  - Consists of DOI personnel whose job functions must incorporate security considerations into lifecycles of systems and programs. This group also includes services support functions such as adding personnel, establishing training and purchasing IT related items.
  - Group membership includes:
    - IT Project/Program Managers
    - Privacy Act Officers
    - Records Management Officials
    - Freedom of Information Act Officials
    - Information Resource Managers
    - Training personnel
    - Human Resources personnel tasked with inducting new personnel
  - If managing any IT related contracts (including personnel), the following collaboration roles also require role-based security training:

[7] Reference for all training groups focus areas: Office of Personnel Management (OPM) 5 CFR Part 930, Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems.

- Contracting Officers
- Contracting Officer's Representatives or Contracting Officer's Technical Representatives (COR/COTRs)
- Procurement, acquisitions and budget personnel who must know procedures for tracking IT purchases and including IT related clauses in procurements, acquisitions and contracts

- Information Security Training Focus Areas – training should include at least 2 of the following:
  - Information Security Basics
  - Management and Implementation level training in:
    - Security Planning
    - System/Application Security Management
    - System Application Life Cycle Management
    - Risk Management
    - Contingency Planning
  - Account Management and Access Controls
  - Configuration Management and Change Control
  - Data Classification and Records Management

- **Group 3 – Information Security Personnel**
  - Consists of DOI personnel whose job functions may include ensuring, evaluating or certifying the confidentiality, integrity, and availability of systems, networks, and data through planning, managing, assessment, analysis, development, implementation, or maintenance.
  - Group membership includes:
    - Chief Information Security Officers (CISOs)
    - Deputy Chief Information Security Officers (DCISOs)
    - Information Assurance Officers (IAOs)
    - Information System Security Officers (ISSOs)
    - Information System Security Managers (ISSMs)
    - Plan of Actions and Milestones (POA&M) Managers and Coordinators
    - Network Administrators
    - Telecommunications Specialists
    - Database Administrators
    - System/Application Administrators (including Internet protective systems, or email system administrators)
    - Systems Operations Personnel (e.g. Network Operations Centers (NOCs) and Security Operations Centers (SOCs) administrators and managers)
    - Computer Incident Response Team/Center members (CIRT/CIRC personnel, including forensic analysts)
    - Technical Support Personnel (e.g. help desk personnel/administrators and managers)
    - IT Security Auditors, Assessors, and Information Assurance Compliance Officers

- IT Security Policy and Compliance – Auditors, Evaluators and Managers

- Information Security Training Focus Areas – training should include at least 2 of the following:
  - Information Security Basics
  - Security Planning
  - System/Application Security Management
  - System Application Life Cycle Management
  - Risk Management
  - Contingency Planning
  - Incident Response
  - Account Management and Access Controls
  - Configuration Management and Change Control
  - Data Classification and Records Management

- **Group 4 – IT Functional Management and Operations Personnel –**
  - Consists of DOI personnel whose job functions include activities that include the design, development, enhancement, implementation, support, or disposal of information systems.
  - Group membership includes:
    - Computer Hardware/Software Engineers
    - System Designers/Developers
    - Programmers/Systems Analysts
    - Data Center Personnel not listed in Group 3
  - Information Security Training Focus Areas – training should include at least 2 of the following:
    - Information Security Basics
    - Management and Implementation Level Training in:
      - Security Planning
      - System/Application Security Management
      - System Application Life Cycle Management
      - Contingency Planning
      - Risk Management
    - Data Classification and Records Management

2.2 Assigning Personnel to Information Security Training Groups

Based on the criteria established within this Standard, supervisors, information security management personnel (e.g. Bureau/Office CISOs), Bureau/Office Training Managers, contract management staff, and HR personnel will coordinate assigning personnel to the training group(s) that best correspond to the individual's current job functions and responsibilities. This assignment process must include all applicable individuals that occupy any of the information security roles, responsibilities or functions identified in Section 2.1 of this Standard.

A record of the Information Security Training Group assigned to each relevant individual shall be maintained as a part of the employee's personnel or training record, as appropriate.

For example:

IT System User Name: "John Smith"
Job Function/Role: "DOI LAN Administrator"
DOI Information Security Training Group: "Information Security Personnel (Group 3)"

2.3 TRAINING TO CONTRACTORS

The DOI RBST requirement is applicable to contractors that support DOI information systems, programs, and missions and that meet the criteria in this guide. Where applicable, Bureaus/Office contract management staff should include contract language in any IT related contracts specifying compliance with DOI annual role-based security training requirements. (See DOI Memorandum *Information Technology Security Requirements for Acquisition,* dated 08-18-2004).

2.4 TRAINING CONTENT

RBST must follow the recommended content guidance outlined in the most current version of NIST Special Publication 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model.*

As outlined by NIST, Information Security training is divided into three fundamental training content categories:

- **Laws and Regulations** – The types of knowledge, skills, behaviors, abilities, and competencies relative to the laws and regulations pertaining to information and asset protection that govern IT management and use of information within the Federal Government. These include government-wide requirements such as the Federal Information Security Management Act (FISMA), policy promulgated by the Office of Management and Budget, standards and guidelines disseminated by NIST, as well as policies and procedures specific to a Department or agency;
- **Security Program** – Competencies relative to the establishment, implementation, and monitoring of an Information Security Program within an organization; and
- **System Life Cycle Security** – Competencies relative to the nature of information security needed throughout each phase of a given system's life cycle. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* identifies five phases in the system life cycle that are typical for an information system: (i) system initiation; (ii) system development and acquisition; (iii) system implementation/assessment; (iv) system operations and maintenance; and (v) system disposal.

Appendix D, RBST Courses by Group, will be updated each fiscal year with available RBST courses within DOI LEARN.

3 DOI ROLE-BASED SECURITY TRAINING, TRACKING AND COMPLIANCE REPORTING

3.1 MANAGEMENT AND TRACKING

Human Resources (HR) within Bureaus and Offices will coordinate with their DOI LEARN Managers and Data Stewards to ensure that employee security training progress is tracked and managed actively within DOI LEARN. Bureau/Office CISOs or designate must review Information Security Training progress reports generated from DOI LEARN to validate the accuracy of those reports before Bureau/Office submission to Cyber Security Division (CSD).

3.2 COMPLIANCE REPORTING

In accordance with Federal regulations referenced in Section 1.4 of this Standard, DOI has a requirement to ensure role-based security training is provided to employees having significant information security responsibilities. The OCIO CSD will examine RBST progress reports from Bureaus and Offices to ensure compliance across the Department, consolidate and report information security training metrics on behalf of the Department.

APPENDIX A – ACRONYMS

This appendix provides a list of acronyms for information security-related terms. It includes those used in this document as well as others of a general nature that may be of interest.

Acronym	Definition
AO	Authorizing Official
BCISO	Bureau Chief Information Security Officer
CISO	Chief Information Security Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
CIRT	Computer Incident Response Team
DAA	Designated Approving/Accrediting Authority
DCIO	Deputy Chief Information Officer
DCISO	Deputy Chief Information Security Officer
DoD	Department of Defense
DOI	Department of the Interior
FISMA	Federal Information Security Management Act
HR	Human Resources
IAO	Information Assurance Officer
IT	Information Technology
ITSP	Information Technology Security Program
ISSO	Information System Security Officer
ISSM	Information System Security Manager
KSA	Knowledge, Skills, Abilities

LAN	Local Area Network
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PM	Program Manager
POA&M	Plan of Actions and Milestones
POC	Point of Contact
RBST	Role-Based Security Training
RITSM	Regional IT Security Manager
SDLC	System Development Life Cycle
SOC	Security Operations Center
SP	Special Publication
SSP	System Security Plan

APPENDIX B – REFERENCES

This appendix provides a list of relevant statutes, regulations, directives, and other guidance applicable to Role-Based Security Training. It includes those cited in this document as well as others of a general nature that may be of interest.

Laws and Office of Management and Budget (OMB) Publications

Public Law 107.347, Title III, Federal Information Security Management Act (FISMA) of 2002, December 17,.2002.

Public Law 104-106, Division E, 40 U.S.C. 1401, Information Technology Management Reform Act (ITMRA) of 1996 (Clinger-Cohen Act), February 10, 1996.

OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, November 28, 2000.

OMB Memorandum 99-20, Security of Federal Automated Information Resources, June 23, 1999.

National Institute of Standards and Technology (NIST) Special Publications

NIST SP 800-16, Rev. 1 (Draft) Information Technology Security Training Requirements: A Role- and Performance-Based Model, March 2009.

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.

NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, Aug 2009.

NIST SP 800-100, Information Security Handbook: A Guide for Managers, October 2006.

Department of the Interior (DOI) Publications

Part 375 Departmental Manual, Chapter 19, Information Technology Security Program, April 15, 2002.

DOI Information Technology Security Policy Handbook.

DOI Memorandum Information Technology Security Requirements for Acquisition, dated 08-18-2004.

Part 370 Departmental Manual, Chapter 752, Discipline and Adverse Actions, December 26, 2006.

Other Publications

OPM 5 CFR Part 930, Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems.
OPM Memorandum dated July 2, 2007, New Standard Form (SF) 182, Authorization, Agreement and Certification of Training Form
OPM 5 CFR Part 410.701(a)(b), Training; Reporting Requirements, Subpart G – Reporting

DoD 8570.01-M, Information Assurance Workforce Improvement Program

APPENDIX C - LISTING OF DOI RECOGNIZED INFORMATION SECURITY PROFESSIONAL CREDENTIALS

- Carnegie Mellon Software Engineering Institute CERT® - Computer Security Incident Handler (CSIH)
- Federated Enterprise Architecture Certification (FEAC) - Certified Enterprise Architect (CEA)
- Information Systems Audit and Control Association (ISACA) Certified Information Systems Auditor (CISA)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified in Risk and Information Systems Control (CRISC)
- International Information Systems Security Certification Consortium $(ISC)^2$ Certification and Accreditation Professional (CAP)
- $(ISC)^2$ Systems Security Certified Practitioner (SSCP)
- $(ISC)^2$ Certified Information Systems Security Professional (CISSP)
- $(ISC)^2$ Certified Secure Software Lifecycle Professional (CSSLP)
- ASIS International Certified Protection Professional (CPP)
- ASIS International Professional Certified Investigator (PCI)
- ASIS International Physical Security Professional (PSP)

Note: These Information Security Professional Credentials were selected for their relevance to Information Security, and their associated annual continuing education requirements for maintenance of these credentials. Suggestions for adding other credentials to this list can be directed to: DOI_IT_Security_Training@ios.doi.gov .

Group 1 - Executive and Senior Management (Minimum 1 per year)

Focus Areas in Blue

To change the Focus Area simply modify Column B with a different number, 1-10, and 'Sort' on Column 'B' only.

1		**Information Security Basics**
1	•	Non-SkillSoft / no-charge: 2010 Computer Security Incident Response Training (CSIRT) Overview (1 hr)
1	•	Protecting and Sharing Excel 2007 Workbooks, mo_expu_a02_dt_enus (2 hrs)
1	•	Introduction to information security, 216913_ENG (1.75 hrs)
1	•	Operational information security, 217983_ENG (1.5 hrs)
1	•	Malicious code and information security, 217043_ENG (1.75 hrs)
1	•	Information security and the Internet, 216960_ENG (1.5 hrs)
2		**Policy Level Security Planning and Management**
2	•	Information Security Governance: Overview, sp_cism_a01_it_enus (2 hrs)
2	•	Information Security Governance: Strategies and Goals, sp_cism_a02_it_enus (2 hrs)
2	•	Information Security Governance: Developing an Action Plan, sp_cism_a03_it_enus (2 hrs)
2	•	Information Security Program Development: Introduction and Roadmap, sp_cism_a06_it_enus (2 hrs)
2	•	Information Security Program Development: Resources, sp_cism_a07_it_enus (2 hrs)
2	•	Information Security Program Development: Metrics and Implementation, sp_cism_a08_it_enus (2 hrs)
2	•	Information Security Program Development: Introduction and Framework sp_cism_a09_it_enus (2 hrs)
2	•	Information Security Program Development: Resources and Implementation, sp_cism_a10_it_enus (2.5 hrs)
3		**Emergency Management and Disaster Recovery**
3	•	Business Continuity and Disaster Recovery Planning, 244085 (140 mins)
4		**Strategic Security Planning or Implementation**
4	•	Information Availability, 240092 (2.5 hrs)
5		**Risk Management Framework**
5	•	Information Risk Management: Program Framework and Risk Assessment, sp_cism_a04_it_enus (2 hrs)
5	•	Information Risk Management: Analysis, Mitigation, and Monitoring, sp_cism_a05_it_enus (2 hrs)
5	•	Approaches to Risk Management, PD0242 (2 hrs)
5	•	Risk Basics, PD0241 (2 hrs)
5	•	Decisions and Risk, PD0243 (2 hrs)
5	•	Risk Assessment and Prevention (HRCI/PHR - 2007-aligned), HR0277 (2.5 hrs)
5	•	Strategic Planning and Risk Management, PD0244 (2.5 hrs)
5	•	Risk Strategies: The Cutting Edge, PD0245 (2.5 hrs)
5	•	Strategic Approaches to Risk Management (HRCI/SPHR - 2007-aligned) (2 hrs)
5	•	Information Security and Risk Management, 243962_ENG (3 hrs)

Foundation Cloud Hosting Services Ordering Guide 2013

Version 1.0
DOI, National Business Center, Acquisition Services Directorate

1. Introduction

The Foundation Cloud Hosting Services contract(s) were competitively awarded by the Department of the Interior (DOI), National Business Center (NBC), Acquisition Services Directorate (AQD) in accordance with Federal Acquisition Regulations (FAR) Parts 12 and 15. These contract(s) were set up in order to provide technical service lines within the infrastructure foundation for developing composite services that will be represented in a "Mission-Facing", DOI-Wide IT Services Catalog offerings at discounted prices and to facilitate ordering of these services. Any and all orders issued against this IDIQ contract(s) shall be in accordance with this ordering guide, FAR 16.505, and any other agency policies and procedures.

1.1 Foundation Cloud Hosting Services Pricing

IDIQ contract holders were required to provide detailed pricing for explicitly defined, standard services, so DOI and other AQD customers can easily compare pricing for service across contract holders. Additional discounts may also be requested and obtained at the order level. Pricing must be either at or below the contractor's IDIQ contract price.

2. List of Awarded Technical Service Lines by Contractor

Services as identified within the contract(s) may be obtained from the contractors with awards for the relevant Service Lines as shown in Table 1, Technical Service Line Awards Per Contractor. For task orders issued against this contract the order request will originate from an AQD Contracting Officer and will identify the scope of work required and any additional instructions regarding submission of quotes.

Technical Service Line → / Vendor ↓	Storage Services	Secure File Transfer Services	Virtual Machine Services	Database Hosting Services	Web Hosting Services	Development and Test Environment Hosting Services	SAP Application Hosting Services
Aquilent	X	X	X	X	X	X	N/A
AT&T	X	X	X	X	X	X	N/A
Autonomic Resources	X	X	X	X	X	X	N/A
CGI	X	X	X	X	X	X	N/A
Global Technology Resources	X	X	X	X	X	X	N/A
IBM	X	X	X	X	X	X	X
Lockheed Martin	X	X	X	X	X	X	N/A
Smartronix	X	N/A	X	X	X	X	X
Unisys	X	X	X	X	X	X	X
Verizon	X	X	X	X	X	X	X

Table 1: Technical Service Line Awards per Contractor

3. Steps to Order

This section provides simple steps necessary to place an order under the Foundation Cloud Hosting Services contract(s).

3.1. Scope Determination

First, determine if the requirement is within scope of the Foundation Cloud Hosting Services contract(s). The following technical service lines are included:

- *Storage Services Technical Services line* includes, but is not limited to Cloud Based Storage Services in support of the DOI Continuity of Operations (CoOP), Disaster Recovery (DR), and Data Center Consolidation Transition Support Requirements.

- *Secure File Transfer Services Technical Services line* includes, but is not limited to an enterprise-wide capability for any employee, contractor or partner working on the DOI network to securely transfer files of any size and type to either internal or external business partners. This includes the capability for DOI employees, contractors and partners to receive files of any size and type from external business partners, while maintaining confidentiality and integrity, and the ability to manage the files in a web environment.

- *Virtual Machine Services Technical Services line* includes, but is not limited to Cloud Based Virtual Machine Services in support of the Data Center Consolidation Transition Support and New Application Implementation Requirements. This Service Line may also be considered as an alternative to technical refresh of physical servers, a quick response

resource to explore innovation opportunities, or rapid response multiprocessor multi-machine simulation environment.

- *Database Hosting Services Technical Services line* includes, but is not limited to, Cloud Based Database Hosting Services in support of the DOI Data Center Consolidation Transition and New Application Implementation Requirements. This service line may include stand-alone databases, shared data sources, or tiered database solutions including components of one or more other Technical Service Lines.

- *Web Hosting Services Technical Services line* includes, but is not limited to cloud Based Web Hosting Services in public, private, community and hybrid cloud environments. This service line may include any combination of other Technical Service lines necessary to deliver static and/or dynamic information to the DOI stakeholders, and includes hosting for an enterprise-wide content management system.

- *Development and Test Environment Hosting Technical Services line* includes, but is not limited to providing a flexible, scalable, on-demand environment to support development, testing, staging, and/or quality assurance before releasing new applications and changes into the DOI production environment. They also support ad-hoc innovation activities. Change Control and User Permissions in this non-production environment are typically established on an instance by instance basis by the authorized user who provisioned the service.SAP Application Hosting Services

3.2. Prepare Statement of Work (SOW) or Statement of Objectives (SOO)

Here are some salient points to consider when drafting requirements:

Scope of work to be performed
Performance objectives, to include any Service Level Agreements specific to the order
Technical requirements
Deliverables, if any

3.3. Period of Performance

The term of the Foundation Cloud Hosting Services contract(s) will be for ten (10) years, base and all option periods are exercised. Contractors may be awarded orders that extend beyond the current term of their contract as long as option periods exist in their contract that, if exercised, will cover the IDIQ contract's period of performance.

3.4. Prepare the Request for Quote (RFQ)

Follow established agency procedures for preparing an RFQ, including any internal policies and procedures related to acquiring IT products and services. Consider the following topics:

3.4.1. Order Value & Funding Type

Estimate the value of the order. Recommend including language, in the RFQ, which indicates the intent to seek additional discounts for orders that are expected to exceed $500,000.

3.4.2. Service Level Agreement (SLA) (Performance Measurements)

Service providers are required to meet the SLA requirements specified in the IDIQ contract(s) and/or as specified in the RFQ for the individual orders. Ordering activities that acquire services through an order against the IDIQ contract(s) can negotiate lower pricing, but the service provider cannot charge prices above the specified prices for a higher level of service.

3.4.3. Evaluation Criteria

Orders can be evaluated either on a best value determination or lowest priced technically acceptable basis. This will be specified within each individual order. For those determined to be evaluated based on best value determination, consider including some combination of technical capability, price, and/or past performance when crafting best value evaluation factors.

3.5. Issue the RFQ

Federal Acquisition Regulation (FAR) Part 16.505 is applicable when issuing the RFQ. RFQs must be issued to all contract holders offering the requested technical service lines in accordance with IDIQ Contract Section H.19, Fair Opportunity Ordering. Additionally, contractors must obtain authorization in accordance with Section J, Attachment 1, Department of the Interior Security Control Standard, Access Control, July 2011, version 1.3, of the IDIQ contract(s).

Allow a reasonable amount of time for IDIQ contract holders to prepare and submit questions regarding the RFQ and to submit quotes. Quotes may be submitted either by fax, email, hand delivered, courier, mail, etc. The method required for delivery shall be specified in the individual RFQs.

3.6. Evaluate

After the RFQ Close Date, evaluate all responses received using the evaluation criteria specified in the RFQ and select the IDIQ contract holder that represents the best value or represents the lowest priced technically acceptable. Notwithstanding the IDIQ contract pricing, it is recommended to request further price reductions when issuing orders under these contracts.

3.7. Award and Award Documentation

In accordance with the IDIQ contract(s), FAR 16.505, and established agency procedures order files shall contain, at a minimum, the following. Additionally, the Government reserves the right to issue orders orally, by facsimile, or by any other electronic commerce methods.

Note the IDIQ contract holder receiving the order & all holders considered to include the approved justification for any exceptions for exclusion of sources

- Description of what was purchased and agreed upon pricing
- The evaluation methodology used in selecting the holder to receive the order
- The rationale for any tradeoffs in making the selection, if applicable
- The price reasonableness determination