OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE U.S. DEPARTMENT OF THE INTERIOR FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2017

This is a revised version of the report prepared for public release.

Report No.: 2016-ITA-052

February 2018

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Memorandum

MAR 0 8 2018

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall Mary L Kendall
Deputy Inspector General

Subject: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2017
Report No. 2017-ITA-052

This memorandum transmits the KPMG LLP (KPMG) Federal Information Security Modernization Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2017. FISMA (Public Law 113-283) requires Federal agencies to have an annual independent evaluation of their information security programs and practices performed. This evaluation is to be performed by the agency's Office of Inspector General (OIG) or by an independent external auditor, as determined by the OIG, to determine the effectiveness of such programs and practices.

KPMG, an independent public accounting firm, performed the DOI FY 2017 FISMA audit under a contract issued by the DOI and monitored by the OIG. As required by the contract, KPMG asserted that it conducted the audit in accordance with Generally Accepted Government Auditing Standards to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. KPMG is responsible for the findings and conclusions expressed in the audit report. We do not express an opinion on the report, nor on KPMG's conclusions regarding DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-18-02, "Fiscal Year 2017–2018 Guidance on Federal Information Security and Privacy Management Requirements," dated October 16, 2017.

KPMG reviewed information security practices, policies, and procedures at the DOI Office of the Chief Information Officer and the following 15 DOI bureaus and offices:

- Bureau of Indian Affairs
- Bureau of Land Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement
- Bureau of Ocean Energy Management
- U.S. Fish and Wildlife Service

- Interior Business Center
- National Park Service
- Office of Natural Resources Revenue
- Office of Inspector General
- Office of the Secretary
- Office of Surface Mining Reclamation and Enforcement
- Office of the Special Trustee for American Indians
- Office of the Solicitor
- U.S. Geological Survey

To ensure the quality of the audit work, we—

- Reviewed KPMG's approach and planning of the audit
- Evaluated the auditors' qualifications and independence
- Monitored the audit's progress at key milestones
- Engaged in regularly scheduled meetings with KPMG and DOI management to discuss audit progress, findings, and recommendations
- Reviewed KPMG's supporting work papers and audit report
- Performed other procedures as deemed necessary

KPMG identified needed improvements in the areas of risk management, configuration management, identity and access management, and information system continuous monitoring. KPMG made 20 recommendations related to these control weaknesses intended to strengthen the Department's information security program, as well as those of the Bureaus and Offices. In its response to the draft report, the Office of the Chief Information Officer concurred with all recommendations and established a target completion date for each corrective action.

We will refer KPMG's recommendations to the Office of Financial Management for audit follow-up. The legislation creating the OIG requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement recommendations; and recommendations that have not been implemented.

We appreciate the cooperation and assistance of DOI personnel during the audit. If you have any questions regarding the report, please contact me at 202-208-5745.

Attachment

The United States Department of the Interior
Office of Inspector General
Federal Information Security Modernization Act of 2014
Fiscal Year 2017 Performance Audit

February 8, 2018

KPMG LLP
1676 International Drive
McLean, Virginia 22102

KPMG LLP
1676 International Drive
McLean, VA 22102

February 8, 2018

Ms. Mary L. Kendall
Deputy Inspector General
U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW MS 4428
Washington, DC 20240-0001

Dear Ms. Kendall:

This report presents the results of our work conducted to address the performance audit objectives relative to the Fiscal Year (FY) 2017 *Federal Information Security Modernization Act of 2014 (FISMA)* Audit for unclassified information systems**.** We performed our work during the period of June 24 to September 30, 2017 and our results are as of November 17, 2017.

We conducted this performance audit in accordance with *Government Auditing Standards.* Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit objective(s) of our work for the year ending September 30, 2017 were to:

- Perform the annual independent FISMA audit of DOI's information security programs and practices related to information systems in accordance with the FISMA, Public Law 113-283, 44 USC 3554.
- Assess the implementation of the security control catalog contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 4. We utilized criteria and guidance, including Federal Information Processing Standard (FIPS) Publication (PUB) 199, FIPS PUB 200, and NIST SP 800-37 Rev 1, to evaluate DOI's implementation of the risk management framework and the extent of implementation of select security controls.
- Prepare responses for each of the Department of Homeland Security (DHS) FY17 FISMA Reporting Metrics on behalf of the DOI Office of Inspector General (OIG), to support documented conclusions with appropriate rationale/justification as to the effectiveness of the information security program and practices of the DOI for each area evaluated and overall.

Our procedures tested security control areas identified in NIST SP 800-53 and additional security program areas identified in the 2017 FISMA Reporting Metrics for the OIG. Our sample was selected from information systems distributed across 15 Bureaus/Offices. These Bureaus/Offices are: the Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Ocean and Energy Management (BOEM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), Interior Business Center (IBC), National Park Service (NPS), Office of Inspector General (OIG), Office of Natural Resources Revenue (ONRR), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), the Office of the Special Trustee for American Indians (OST), Office of the Solicitor (SOL), and the U.S. Geological Survey (USGS). At the conclusion of our test procedures, we aggregated the individual bureau and information system results by control area to produce results at the Department level.

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53 Revision 4. DOI has established security training, incident response and contingency planning programs. We identified needed improvements in areas audited including risk management, configuration management, identity and access management, and information system continuous monitoring.

The following table summarizes the control areas tested and the control deficiencies identified in the fiscal year 2017 FISMA Reporting Metrics for the OIG.

Cybersecurity Framework Security Functions[1]	Summary of Results
1. Identify (Risk Management)	DOI has established a risk management program. However, DOI has not fully: • Implemented newly adopted risk management policies and procedures at BOEM and BSEE; • Formally developed an enterprise architecture at BSEE and BOEM; • Designed and implemented a security architecture at the business process and system information levels across three bureaus and offices: BOEM, BSEE, and NPS; • Designed and implemented management dashboards to facilitate a centralized view of all sources of risk at the BSEE, BOEM, USGS, and NPS; • Implemented a process to [redacted] are fully implemented in accordance with DOI policy at the FWS; • Reviewed [redacted] at FWS to ensure [redacted]; • Disabled [redacted] at FWS; and • Implemented a process to ensure that open Plan of Action and Milestones (POA&M) are reviewed and maintained in accordance with DOI policy at BLM and SOL.
2. Protect (Configuration Management, Identity and Access Management, and Security Training)	DOI has established configuration management, identity, access management, and security training programs. However, DOI has not fully: • Implemented a process to [redacted] at OST's contractor location;

[1] Metrics organized around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover.

	• Documented procedures for maintaining [redacted] at BOR; • Maintained evidence to support physical security access logs are periodically reviewed at BLM; • [redacted] reviews at BLM; • Implemented a process to [redacted] at BLM [redacted] • Effectively [redacted] BLM; and • Implemented a process to ensure information system access is authorized after supervisor approval at OST.
3. Detect (Information Security Continuous Monitoring)	DOI has established an information security continuous monitoring program. However, DOI has not fully: • Implemented newly adopted ISCM strategy at BOEM and BSEE; • Defined lessons learned in the ISCM strategy in order to identify opportunities for improvement at BOEM and BSEE; and • Defined performance measures to evaluate the effectiveness of the ISCM program at BOEM and BSEE.
4. Respond (Incident Response)	DOI has established an incident response program.
5. Recover (Contingency planning)	DOI has established a contingency planning program.

We have made 20 recommendations related to these control weaknesses intended to strengthen the respective Bureaus, Offices, and the Department's information security program. In addition, the report includes five appendices. Appendix I summarizes the program areas in which bureaus and offices have control deficiencies, Appendix II provides a list of acronyms, Appendix III provides the status of FY16 recommendations, Appendix IV lists the NIST Special Publication 800-53 security controls cross-referenced to the Cybersecurity Framework, and Appendix V provides the Responses to the Department of Homeland Security FISMA 2017 questions for Inspector Generals.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not render an opinion on the U.S. Department of the Interior's internal controls over financial reporting or over financial management systems. KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

KPMG LLP

The United States Department of the Interior
Office of Inspector General
Federal Information Security Modernization Act of 2014 - Fiscal Year 2017 Performance Audit

Table of Contents

Background

Mission of the DOI and its Bureaus/Offices

The U.S. Department of the Interior (DOI) protects America's natural resources and heritage, honors our cultures and tribal communities, and supplies the energy to power our future. DOI is composed of a number of Bureaus and a number of additional Offices that fall under the Office of the Secretary, the Assistant Secretary for Policy, Management and Budget, Solicitor's Office and Office of Inspector General. Of those, the following 15[2] Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2017:

1 The **Bureau of Indian Affairs (BIA)** is responsible for the administration and management of 55 million surface acres and 57 million acres of subsurface minerals estates held in trust by the United States for American Indian, Indian tribes, and Alaska Natives.

2 The **Bureau of Land Management (BLM)** administers 262 million surface acres of America's public lands, located primarily in 12 Western States. The BLM sustains the health, diversity, and productivity of the public lands for the use and enjoyment of present and future generations.

3 The **Bureau of Ocean and Energy Management (BOEM)** manages development of U.S. Outer Continental Shelf energy and mineral resources in an environmentally and economically responsible way.

4 The **Bureau of Reclamation (BOR)** manages, develops, and protects water and related resources in an environmentally and economically sound manner in the interest of the American public.

5 The **Bureau of Safety and Environmental Enforcement (BSEE)** is responsible for overseeing the safe and environmentally responsible development of energy and mineral resources on the Outer Continental Shelf.

6 The **U.S. Fish and Wildlife Service (FWS)** was created to conserve, protect, and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people.

7 The **National Park Service (NPS)** supports to preserve unimpaired the natural and cultural resources and values of the national park system, a network of nearly 400 natural, cultural, and recreational sites across the nation, for the enjoyment, education, and inspiration of this and future generations.

8 The **Interior Business Center (IBC)** provides the executive leadership, policy, guidance, independent program evaluation, and coordination needed to manage the diverse, complex, nationally significant programs that are DOI's responsibility.

9 The **Office of Inspector General (OIG)** accomplishes its mission by performing audits, investigations, evaluations, inspections, and other reviews of the DOI's programs and operations. They independently and objectively identify risks and vulnerabilities that directly affect, or could affect, DOI's mission and the vast responsibilities of its bureaus and entities. Their objective is to improve the accountability of DOI and their responsiveness to Congress, the Department, and the public.

10 The **Office of Natural Resources Revenue (ONRR**) collects, accounts for, and verifies natural resource and energy revenues due to States, American Indians, and the U.S. Treasury.

[2]. Our sample resulted in a subset of information systems distributed over 14 Bureaus/Offices.

11 The **Office of the Secretary (OS)** is primarily responsible for providing quality services and efficient solutions to meet DOI business needs through its most important asset – its people.

12 The **Office of Surface Mining (OSMRE)** carries out the requirements of the Surface Mining Control and Reclamation Act in cooperation with States and Tribes. Their primary objectives are to ensure that coal mines operate in a manner that protects citizens and the environment during mining and assures the land is restored to beneficial use following mining, and to mitigate the effects of past mining by aggressively pursuing reclamation of abandoned coalmines.

13 The **Office of the Special Trustee for American Indians (OST)** improves the accountability and management of Indian funds held in trust by the federal government.

14 The **Office of the Solicitor (SOL)** performs the legal functions for the United States Department of the Interior, manages the Department's Ethics Office, and resolves FOIA Appeals.

15 The **U.S. Geological Survey (USGS)** serves the nation by providing reliable scientific information to describe and understand the earth; minimize loss of life and property from natural disasters; manage water, biological, energy, and mineral resources; and enhance and protect our quality of life.

Information Technology (IT) Organization

The Office of the Chief Information Officer (OCIO) heads the security management program for the Department. The Chief Information Officer (CIO) heads the OCIO. The CIO reports to the Secretary and receives operation guidance and support from the Assistant Secretary – Policy, Management and Budget through the Deputy Assistant Secretary – Technology, Information, and Business Services.

The Senior Associate CIO reports to the CIO and serves as the OCIO’s primary liaison to bureau Associate CIOs for day-to-day interactions between bureau leadership and OCIO’s major functions.

The DOI Chief Information Security Officer (CISO) reports to the CIO and oversees the Information Assurance Division. The Division is responsible for IT security and privacy policy, planning, compliance and operations. The division provides a single point of accountability and visibility for cybersecurity, information privacy and security.

The OCIO’s mission and primary objective is to establish, manage, and oversee a comprehensive information resources management program for the Department of the Interior. A stable and secure information management and technology environment is critical for achieving the Department’s mission.

FISMA

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency Inspector General (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. The fiscal year 2017 FISMA metrics were aligned with the five function areas in the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect. Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides Inspector Generals with guidance for assessing the maturity of controls to address those risks.

Objective, Scope, and Methodology

The objectives for this performance audit for the year ending September 30, 2017:

- Perform the annual independent Federal Information Systems Security Modernization Act of 2014 (FISMA) audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 113-283, 44 USC.
- Assess the implementation of the security control catalog contained in the NIST SP 800-53 Rev 4. We utilized criteria and guidance, including FIPS 199, FIPS 200, and NIST SP 800-53 Rev 4, to evaluate the implementation of the risk management framework and the extent of implementation of security controls selected from the security control catalog. The table in Appendix IV lists the NIST SP 800-53 revision 4 controls considered during the performance audit.
- Prepare responses for each of the OMB/Department of Homeland Security (DHS) FISMA Reporting Metrics on behalf of the DOI OIG, to support documented conclusions on the effectiveness of the information security program and practices of the DOI for each area evaluated.

The scope of our audit included the following:

- An inspection of relevant information security practices and policies established by the DOI Office of the Chief Information Officer (OCIO) as they relate to the FY2017 OIG FISMA reporting metrics; and
- An inspection of the information security practices, policies, and procedures in use across 15 Bureaus and Offices identified by the DOI OIG, specifically BIA, BLM, BOR, BSEE, BOEM, FWS, NPS, IBC, OIG, ONRR, OS, OSMRE, OST, SOL, and USGS.

Specifically, our approach followed two steps:

Step A: Department and Bureau level compliance – During this step, we gained Department and Bureau understanding of the FISMA-related policies and guidance established by the DOI OCIO. We examined the policies, procedures, and practices established to the applicable Federal laws and criteria to evaluate whether the Department and Bureaus are generally consistent with FISMA.

Step B: Assessment of the implementation of select security controls from the NIST SP 800-53 revision 4. During this process, we assessed the implementation of a selection of security controls from the NIST SP 800-53 Rev 4 for our representative subset (10 %) of DOI's information systems.[3] The controls selected addressed areas covered by the DHS FY2017 Inspector General FISMA Reporting Metrics.

[3] In accordance solicitation order number D17PD00184 with the U.S. Department of the Interior, Office of the Inspector General Financial Audit Services, dated January 13, 2017, we employed a random sampling approach to determine a representative subset of 10 percent of the DOI information systems. That representative subset includes Major Applications and General Support Systems with Federal Information Processing Standard (FIPS) 199 security categorizations of "Low," "Moderate," and "High". The FIPS 199 ratings are defined by the DOI system owner and authorizing official. We randomly selected 15 of 125 operational systems of the total DOI information systems recorded in its official repository, the Cyber Security Assessment and Management tool (CSAM).

The DOI Statement of Work (SOW) for the FISMA audit required us to perform our procedures on a subset of systems defined by the Department for at least 10% of the information systems in the DOI's authoritative information system inventory in the Cyber Security Assessment and Management (CSAM) application. The table below identifies the information systems audited. Those systems are described in Table 1.

Table 1. DOI Information Systems Audited

BUREAU OF INDIAN AFFAIRS			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Moderate	[redacted]

BUREAU OF LAND MANAGEMENT			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Moderate	[redacted]

BUREAU OF RECLAMATION			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Moderate	[redacted]

BUREAU OF OCEAN ENERGY MANAGEMENT			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Low	[redacted]

BUREAU OF SAFETY AND ENVIRONMENTAL ENFORCEMENT			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Moderate	[redacted]

U.S. FISH AND WILDLIFE SERVICE			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	[redacted]	[redacted]

INTERIOR BUSINESS CENTER			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Moderate	[redacted]

NATIONAL PARK SERVICE			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	[redacted]	[redacted]

OFFICE OF NATURAL RESOURCES REVENUE			
System Name	**CSAM ID**	**FIPS 199 Category**	**Type**
[redacted]	[redacted]	Moderate	[redacted]

OFFICE OF INSPECTOR GENERAL			
System Name	CSAM ID	FIPS 199 Category	Type
[redacted]	[redacted]	Moderate	[redacted]

OFFICE OF THE SECRETARY			
System Name	CSA M ID	FIPS 199 Category	Type
[redacted]	[redacted]	Moderate	[redacted]

OFFICE OF SURFACE MINING			
System Name	CSAM ID	FIPS 199 Category	Type
[redacted]	[redacted]	Moderate	[redacted]

OFFICE OF THE SPECIAL TRUSTEE FOR AMERICAN INDIANS			
System Name	CSAM ID	FIPS 199 Category	Type
[redacted]	[redacted]	Moderate	[redacted]

OFFICE OF THE SOLICITOR			
System Name	CSAM ID	FIPS 199 Category	Type
[redacted]	[redacted]	Moderate	[redacted]

U.S. GEOLOGICAL SURVEY			
System Name	CSA M ID	FIPS 199 Category	Type
[redacted]	[redacted]	Moderate	[redacted]

Results of Review

Our procedures identified improvements needed in the areas of risk management, configuration management, identity and access management, and information system continuous monitoring. The details of the weaknesses we identified are as follows.

1. Implementation of the Risk Management program.

KPMG performed the following procedures and noted the following weaknesses in six of 15 bureaus and offices' risk management programs: BSEE, BOEM, USGS, NPS, FWS, and SOL.

BSEE and BOEM:

KPMG inquired of BSEE and BOEM personnel responsible for managing the joint BSEE and BOEM risk management program, which included the BSEE Associate Chief Information Security Officer (ACISO) and the Information System Continuous Monitoring (ISCM) Lead. KPMG also reviewed the BSEE Information System Continuous Monitoring (ISCMP) Plan for Information Technology (IT) Security and Privacy, dated June 28, 2017. The ISCMP includes risk management policies and activities. KPMG noted the following control deficiencies in the BSEE and BOEM risk management program:

1. Risk management policies, procedures and strategy at the enterprise, business process and information system levels were not fully implemented.

2. An enterprise architecture had not been formally developed.

3. The organizations have not fully implemented a security architecture across the enterprise, business processes and information system levels.

4. The organizations have not implemented a management dashboard to facilitate a centralized view of all sources of risk.

USGS:

KPMG inquired of the USGS information security personnel, which included the Information Security Office Compliance Team, Accreditation and Authorization Manager and Plan of Action and Milestones Coordinator responsible for managing the USGS Risk Management Program. KPMG also reviewed Information Security Office Standard Operating Procedures for Program Management (PM) dated July 2017. KPMG noted USGS lacked a management dashboard to facilitate a centralized view of all sources of risk.

NPS

KPMG inquired of National Park Service (NPS) personnel responsible for managing the joint NPS Risk Management program, which included the NPS Deputy Chief Information Security Officer (DCISO) and NPS National Information System Center (NISC) Information Technology (IT) Security Officer. KPMG also reviewed the NPS Information System Continuous Monitoring Plan for Information Technology (IT) Security and Privacy dated July 15, 2017. The ISCMP includes risk management policies and activities. KPMG noted the following control deficiencies in the NPS risk management program:

1. NPS had not fully implemented a security architecture across the enterprise, business processes and information system levels.

2. NPS did not implement a management dashboard to facilitate a centralized view of all sources of risk.

FWS:

KPMG conducted vulnerability security scans over a selection of [redacted] computing environment consists of nine (9) regions and KPMG judgmentally selected five (5) regions to evaluate. KPMG identified 665 of 946 (70%) network devices with 643 [redacted] were not remediated in accordance with DOI Security Control Standards.

[redacted]

Additionally, [redacted] unless otherwise approved by the CIO. KPMG informed FWS management of the condition and provided detailed results of testing. Upon notification, FWS proactively coordinated efforts to remediate the devices with [redacted].

Furthermore, during the course of the audit, it was determined that the FWS [redacted], was not configured properly. KPMG informed management of the misconfiguration and FWS management corrected the misconfiguration. KPMG later confirmed management's corrective actions were effective.

SOL:

KPMG was informed that SOL has an agreement with the OCIO's branch of Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM) for management services. These responsibilities include conducting annual control reviews, POA&M management, and security documentation updates.

KPMG noted the following control deficiencies with SOL's Plan of Action and Milestones (POA&M) process:

- SOL management was unable to provide evidence that open POA&Ms are updated or reviewed at least quarterly.
- SOL has not effectively reviewed and updated open POA&Ms to reflect current conditions. Specifically, we noted missing milestone information and due dates, multiple delayed milestones with statuses of outstanding weakness completion verification forms (WCVF) that had not been completed or were awaiting Authorizing Official signature as the final milestone step, and slipped milestone dates.
- KPMG judgmentally selected 15 of 163 open POA&Ms to evaluate the quality of the POA&M, and determined that 15 of 15 were not properly maintained, as outlined in Table 2 as follows:

Table 2: List of POA&Ms that were not effectively maintained.

#	POA&M ID	Weakness Description	Status	Workflow Status Date	Due Date
1	[redacted]	[redacted]	Delayed	12/15/2009	06/25/2010
2	[redacted]	[redacted]	Delayed	11/10/2010	11/26/2010
3	[redacted]	[redacted]	Delayed	11/10/2010	11/26/2010
4	[redacted]	[redacted]	Delayed	11/10/2010	1/28/2011
5	[redacted]	[redacted]	In Progress	1/18/2011	N/A
6	[redacted]	[redacted]	In Progress	1/19/2011	N/A
7	[redacted]	[redacted]	In Progress	1/19/2011	N/A
8	[redacted]	[redacted]	In Progress	1/19/2011	N/A
9	[redacted]	[redacted]	In Progress	1/20/2011	N/A
10	[redacted]	[redacted]	Delayed	1/20/2011	12/19/2012
11	[redacted]	[redacted]	In Progress	3/19/2012	N/A
12	[redacted]	[redacted]	Delayed	1/27/2011	03/30/2012
13	[redacted]	[redacted]	Delayed	1/27/2011	02/20/2013
14	[redacted]	[redacted]	Delayed	11/30/2011	01/27/2012
15	[redacted]	[redacted]	Not Started	11/30/2011	N/A

BLM:

The BLM does not consistently update POA&MS on a quarterly basis. Nine POA&M IDs, [redacted] contained in CSAM were created more than one year ago and are in "Draft – Created" workflow status or "Not Started" status, with no dates entered, are not assigned to a user, and/or do not have milestone details entered.

In addition, POA&M ID #[redacted] created on 9/28/16 for the [redacted], is in "Draft – Created" workflow status. This POA&M was reviewed on 3/15/17 and 8/21/17; however, the POA&M is not started, does not contain due dates or an approved status, has no milestones entered, and no updates provided.

The DOI Security Control Standard and NIST SP 800-53, revision 4: PM-7 ENTERPRISE ARCHITECTURE, states: “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.”

The DOI Security Control Standard and NIST SP 800-53, revision 4: PL-8 INFORMATION SECURITY ARCHITECTURE, states: “Control: The organization:

a. Develops an information security architecture for the information system that:

1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and

3. Describes any information security assumptions about, and dependencies on, external services;

b. Reviews and updates the information security architecture at least annually to reflect updates in the enterprise architecture; and

c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.”

NIST SP 800-137 Appendix D-11, D.2.2 MANAGEMENT DASHBOARDS, states:
“A security management dashboard (or security information management console) consolidates and communicates information relevant to the organizational security status in near real-time to security management stakeholders. Personnel with responsibility for information security range from a technical system administrator, to the SISO, to the risk executive (function). The security management dashboard presents information in a meaningful and easily understandable format that can be customized to provide information appropriate to those with specific roles and responsibilities within the organization.

To maximize the benefits of management dashboards, it is important to obtain acceptance and support from upper-level management, define useful and quantifiable organization-specific performance metrics that are based on information security policies and procedures, and ensure the availability of meaningful performance data.“

Department of the Interior, Security Control Standard, Risk Assessment, version 4.1, dated September 2016, RA-5 Vulnerability Scanning states: “Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications System Owner-defined frequency and/or randomly in accordance with organization-defined process, but at least monthly, and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;

2. Formatting checklists and test procedures; and

3. 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 System Owner-defined personnel or roles to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Control Enhancement RA-5 (5) Vulnerability Scanning | Privileged Access

The information system implements privileged access authorization to System Owner-identified information system components for selected System Owner-defined vulnerability scanning activities."

Department of the Interior, Security Control Standard, System and Information Integrity, version 4.1, dated September 2016, SI-2 Flaw Remediation states: "Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Installs security-relevant software and firmware updates within System Owner-defined time period, not to exceed thirty days, of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process."

Department of the Interior, Security Control Standard, Configuration Management, version 4.1, dated September 2016, CM-7 Least Functionality states: "Control: The organization:

a. Configures the information system to provide only essential capabilities; and

b. 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, and FTP (Unless Approved by DOI CIO)."

Department of the Interior, Security Control Standard, Security Assessment, version 4.1, dated September 2016, CA-5 Plan of Action and Milestones states: "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."

Department of the Interior, Security Control Standard, Program Management, version 4.1, dated September 2016, PM-4 Plan of Action and Milestones Process states: "Control: The organization:

> a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
>
> > 1. Are developed and maintained;
> >
> > 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
> >
> > 3. Are reported in accordance with OMB FISMA reporting requirements.
>
> b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions."

BSEE and BOEM had very recently approved a new Information System Continuous Monitoring (ISCM) strategy on June 28, 2017, which includes a detailed risk management process and procedures for elevating triggered events to successively higher management levels based on determinations of extent of risk, including to information system owners, mission and business process owners, and top Bureau management, but had not fully implemented the ISCM Strategy and risk management processes prior to the audit.

BSEE and BOEM management had not taken steps to develop an enterprise architecture.

BSEE, BOEM, and NPS management had not taken steps to develop an information security architecture across the enterprise, business process and system levels.

BSEE, BOEM, and NPS management had not taken steps to develop a dashboard to facilitate a centralized view of all sources of risk, because it was awaiting the Department to provide an Enterprise-level dashboard as part of the department-wide Continuous Diagnostics and Mitigation (CDM)[4] program.

USGS and NPS management had not taken steps to develop and implement a dashboard to facilitate a centralized view of all sources of risk, because it was awaiting the Department to provide an Enterprise-level dashboard as part of the department-wide CDM program.

FWS management did not properly configure the vulnerability scanning tool to scan for vulnerabilities utilizing valid administrative level credentialed security scans to allow a more

[4] CDM is an approach to protect the cybersecurity of the DOI networks and systems. CDM provides the capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate significant risks. Congress established the CDM program to provide adequate, risk-based, and cost effective cybersecurity resources the federal departments and agencies.

effective and accurate method for collecting information of the network and systems. Therefore, [redacted] were not properly identified in a timely manner and not consistently implemented in order to meet the 30-day requirement of remediation for [redacted]

Due to SOL management oversight, POA&M tracking of reviews and updates was not properly maintained for the [redacted].

BLM does not have an adequate process in place to ensure POA&Ms are updated quarterly and are actively managed.

BSEE, BOEM, and NPS: Lack of an Information Security Architectures across the enterprise, business process and information system levels, placement of protection mechanisms and security safeguards might be less effective in protecting information resources.

BSEE, BOEM, NPS, and USGS: Lack of a management dashboard to facilitate a centralized view of all sources of risk, risk management processes, and risk-based decisions made by individuals with significant security responsibilities could be less effective.

BSEE and BOEM: Without knowledge of ISCM activities that are the underlying basis for the BSEE and BOEM risk management process, risk-based decisions made by individuals with significant security responsibilities could be less effective.

BSEE, BOEM, and NPS: Lack of an enterprise architecture and resulting information security architectures across the enterprise, business process and information system levels, placement of protection mechanisms and security safeguards might be less effective in protecting information resources.

FWS [redacted] that can lead to increased risk to the FWS computing environment, which is vital to FWS's mission. The organizational risks could lead to potential [redacted]

SOL: Lack of reviewing, updating, and reporting of POA&Ms can result in weaknesses and vulnerabilities not being appropriately addressed to effectively monitor the progress of corrective efforts for security weaknesses found in the SOL computing environment.

BLM: Failing to remediate or update POA&Ms results in unaddressed weaknesses and outstanding vulnerabilities that could negatively impact BLM's systems and mission and business functions.

We recommend:

1. BSEE and BOEM continue to fully implement risk management processes consistent with the approved ISCM strategy;
2. BSEE, BOEM, and NPS develop an enterprise architecture and subsequent information security architecture across the bureau, business process and system levels;
3. BSEE, BOEM, NPS, and USGS, either independently or in coordination with the Department, implement a management dashboard to facilitate a centralized view of all sources of risk, risk management processes, and risk-based decisions;

4. FWS enhance [redacted] to ensure all relevant and appropriate [redacted] in accordance with DOI policy. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying [redacted];
5. FWS enhance the vulnerability management process to periodically review [redacted], to ensure that [redacted] within the FWS computing environment;

6. SOL enforce oversight compliance to ensure that all responsible parties are effectively reviewing, updating, and maintaining open POA&Ms in CSAM; and

7. BLM develop and enforce a process to ensure POA&Ms are fully defined and updated at least quarterly. POA&Ms should be approved and include milestones, dates, and reasons when delays are encountered.

2. Implementation of the Information System Continuous Monitoring Program.

KPMG performed the following procedures and noted the following weaknesses at two of 15 bureaus and offices, BSEE and BOEM, in implementing their respective information system continuous monitoring programs.

BSEE and BOEM:

KPMG inquired of BSEE and BOEM personnel responsible for managing the joint BSEE and BOEM Information System Continuous Monitoring (ISCM) program, which included the BSEE Associate Chief Information Security Officer (ACISO) and the Information System Continuous Monitoring (ISCM) Lead. KPMG also reviewed the BSEE Information System Continuous Monitoring (ISCMP) Plan for Information Technology (IT) Security and Privacy, dated June 28, 2017. KPMG noted the following control deficiencies in the BSEE Information Continuous Monitoring Program:

1. The recently approved ISCM strategy was not fully implemented across the BSEE and BOEM organizations and information systems;

2. Lessons learned were defined in the ISCM strategy in order to identify opportunities for improvement, but not maintained; and

3. Performance measures to evaluate the effectiveness of the ISCM program were defined, but data supporting metrics were not collected and analyzed.

DOI CIO “Memo Re Ongoing A-A Through Continuous Monitoring”, dated March 16, 2012 states: “Bureaus and Offices are now required to conduct ongoing system authorizations based upon continuous monitoring that assess security controls and analyze organizational risks with a frequency sufficient to support risk-based security decisions to adequately protect organization information, New systems are still required to have all applicable security controls fully assessed prior to Authorizing Official (AO) granting an initial Authorization to Operate (ATO).

The AOs are required to:

- Conduct continuous monitoring of their respective information systems and shall utilize, to the extent practicable, common shared enterprise-wide capabilities to help achieve standardization, cost-efficiencies, and overall program effectiveness of controls across the agency;
- Monitor the security state of their systems on an ongoing basis with a frequency sufficient to make ongoing risk-based decisions on whether to continue to operate the systems within their purview; and
- Develop, document and formally approve a continuous monitoring program for their information systems.”

DOI Security Control Standards and NIST SP 800-53 revision 4 dated April 2013 with updates as of January 22, 2015, Security Assessment and Authorization control family states:

“Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of *System Owner-defined metrics* to be monitored;

b. Establishment of *System Owner-defined freq*uencies for monitoring and *System Owner-defined freq*uencies for assessments supporting such monitoring;

> c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
>
> d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
>
> e. Correlation and analysis of security-related information generated by assessments and monitoring;
>
> f. Response actions to address results of the analysis of security-related information; and
>
> g. Reporting the security status of organization and the information system to the Authorizing Official at least quarterly."

BSEE and BOEM approved a new extensive Information System Continuous Monitoring (ISCMP) Plan for Information Technology (IT) Security and Privacy on June 28, 2017, and did not have adequate time to fully implement the new ISCM Strategy, conduct lessons learned activities, or collect and analyze performance metrics prior to the audit.

Without knowledge of ISCM activities, risk-based decisions made by individuals with significant security responsibilities could be less effective.

Without data and information for the newly defined ISCM qualitative and quantitative performance measures and data from collecting and considering lessons learned, individuals with significant security responsibilities may have difficulty in assessing the effectiveness of the ISCM program in controlling ongoing risk, and in assessing whether there is a need to modify ISCM processes.

We recommend:

8. BSEE and BOEM continue to fully implement the ISCM strategy across both organizations and respective information systems; and
9. BSEE and BOEM consistently maintain data for the qualitative and quantitative performance measures defined in the ISCM strategy and lessons learned meetings, and periodically assess the effectiveness of BSEE and BOEM's ISCM program and identify areas for improvement, as required.

3. Implementation of the Identity and Access Management Program.

KPMG performed the following procedures and noted the following weaknesses at two of 15 bureaus and offices, OST and BLM, regarding implementation of their respective identity and access management programs.

OST:

KPMG inquired of OST management, and was informed that [redacted]

BLM:

BLM does not effectively employ [redacted]

[redacted]

[redacted]

KPMG inspected evidence and noted that [redacted] showing changes in users' [redacted] access. When a need arises, logs can be obtained and reviewed to show all actions performed by privileged users; [redacted]. BLM management was unable to provide requested information above.

Additionally, KPMG inspected [redacted] noting that some [redacted], who fall outside of the [redacted], have the ability to [redacted] though it is not appropriate for them to perform this function. KPMG also inspected BLM's draft [redacted] and noted that BLM is in the process of defining, standardizing, and documenting [redacted].

BLM also does not perform [redacted]

Management informed us that [redacted] a system-monitoring tool, is used to provide an alert to the account management team when a new user account is created. A subsequent review is performed to ensure the newly created account is created by someone on the [redacted]. This process helps mitigate the risk of accounts being created inappropriately when IT staff are centralized.

BLM has developed a process to alert whenever a new user is added to a privileged group, to enforce more scrutiny on the approvals required to obtain access to a privileged group, and ensure the access was approved from the owner of the privileged group. [redacted]

BLM does not formally define the procedures or conditions [redacted]

[redacted] was not documented.

KPMG performed additional testing to determine whether [redacted] KPMG selected a sample of 25 [redacted] to determine whether [redacted].

Exceptions were found for 10 of 25 [redacted] four of 10 [redacted] For six of 10 [redacted] Of these six:

[redacted]

DOI Security Control Standard Access Control, Version 4.1, AC-2, states:

> “<u>Applicability:</u> All Systems
>
> <u>Control:</u> The organization requires approvals by organizational account managers for requests to create information system accounts.”
>
> “f. Creates, enables, modifies, disables, and removes information system accounts in accordance with *System Owner-defined procedures or conditions*;”

DOI Security Control Standard Access Control, version 4.1, AC-6 LEAST PRIVILEGE, states:

> “<u>Applicability:</u> All systems
>
> <u>Control</u>: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.”

OST - OST was not aware that system access needed to be approved prior to access being granted.

BLM – In fiscal year 2014, BLM centralized their IT staff and as a result, are working to [redacted] This effort is taking place zone by zone and while BLM states that most zones [redacted], one of six zones [redacted].

BLM does not have an adequate process in place to ensure that [redacted] in a timely manner [redacted]

When BLM receives the [redacted]

OST - The potential effect is that [redacted]

BLM - [redacted]

[redacted]

We recommend:

10. OST develop a process to ensure supervisors approve access requests prior to providing logical access to the [redacted]
11. BLM restrict [redacted]
12. BLM consider using [redacted]
13. BLM implement a process to perform [redacted] identified during the review are made appropriately and that an analysis is performed to investigate [redacted]
14. BLM implement other methods to [redacted] where possible, such as:
    a. Limiting the functions [redacted]
    b. Limiting the duration [redacted]
    c. Maintaining and reviewing [redacted]

15 [redacted]

16. BLM implement a process to disable or remove [redacted]

4. Implementation of the Configuration Management Program.

During our procedures, KPMG noted the following weaknesses at three of 15 bureaus and offices, OST, BOR, and BLM implementation of their respective configuration management programs.

OST:

> OST's [redacted], does not consistently perform [redacted]

BOR:

> BOR maintains a [redacted]; however, BOR's procedural documents for configuration management do not adequately define and document the process to be followed for maintaining [redacted]
>
> - Roles and responsibilities;
> - Technology utilized;
> - Processes followed to [redacted];
> - Frequency with which the [redacted] will be reviewed and updated, and
> - Process to [redacted]

BLM:

> The [redacted] physical and environmental procedures as defined in the [redacted] system security plan as control PE-06 state that BLM reviews [redacted] and upon occurrence of reportable events or potential indications of events, and requires that copies of the reviews are [redacted]. Through inquiry of management, KPMG was informed that [redacted] However, BLM management was unable to provide evidence [redacted]
>
> We observed evidence o [redacted] however, we could not obtain other evidence of [redacted]
>
> DOI Security Control Standard Physical and Environmental Protection, Version 4.1, PE-6 MONITORING PHYSICAL ACCESS, states:
>
> > "Applicability: All Information Systems
> >
> > Control: The organization:
> >
> > a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
> >
> > b. Reviews physical access logs at least semi-annually and upon occurrence of detected physical security events or potential indications of events; and
> >
> > c. Coordinates results of reviews and investigations with the organizational incident response capability."

DOI Security Control Standard Contingency Planning, Version 4.1, CM-1 Configuration Management Policy and Procedures states:

> "Control: The organization:
>
> a. Develops, documents, and disseminates to all relevant parties:
>
>   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
>
>   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
>
> b. Reviews and updates, as needed, the current:
>
>   1. Configuration management policy, at least every two years; and
>
>   2. Configuration management procedures, at least every two years."

OST - The [redacted] in place at the [redacted] is outdated and cannot easily generate the logs necessary to perform a review. Additionally, this control is a new requirement with the implementation of NIST SP 800-53 rev.4.

BOR – BOR places reliance on the DOI Security Control Standards for Configuration Management Policy and entrusts personnel to follow their own procedures to meet the policy requirements for maintaining the hardware and software inventories. Procedures are not documented and shared with personnel to ensure all are aware of the process to consistently meet the policies.

BLM - BLM's procedures for monitoring physical security access are not being followed as stated in the [redacted] System Security Plan Implementation Statement for control PE-6. Additionally, the documented procedures do not accurately describe the process that was communicated to KPMG. The requirement to review physical security access audit logs is a new requirement with the implementation of NIST SP 800-53 rev.4.

OST - Lack of [redacted] may go undetected, leading to the [redacted].

BOR- Lack of [redacted] may result in [redacted]

BLM – Lack of [redacted]

We recommend:

17. OST update the [redacted] system to the most current version, implement a process to review [redacted] of the [redacted]

18. BOR develop procedure documentation for defining and maintaining [redacted] At a minimum, the procedure document should include the following elements:

- Roles and responsibilities;
- Technology and processes to maintain a complete and accurate inventory;

- Frequency with which the information system component inventory will be reviewed and updated, and
- Process to remove unauthorized, inappropriate, or end of life hardware and software from the system once identified.

19. BLM update system security plans [redacted] to reflect the process in place [redacted]
20. BLM ensure that [redacted]

Conclusion

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53 Revision 4. We identified needed improvement in the areas of risk management, configuration management, identity and access management, and information system continuous monitoring.

Management Response to Report

The following is the Department responses to the report recommendations with targeted completion dates.

Recommendation 1:
BSEE and BOEM concur with recommendation 1. BSEE and BOEM will continue to implement and monitor their June 28, 2017, Information System Continuous Monitoring (ISCM) Strategy and periodically assess its effectiveness.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

Recommendation 2:

BSEE and BOEM concur with recommendation 2. BSEE and BOEM will develop an enterprise architecture (PM-7) and information security architecture (PL-8) that satisfies both i) the DOI Security Control Standard and ii) NIST SP 800-53, revision 4.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

NPS concurs with recommendation 2. NPS will develop an enterprise architecture (PM-7) and information security architecture (PL-8) that satisfies both i) the DOI Security Control Standard and ii) NIST SP 800-53, revision 4.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

Recommendation 3:

BSEE and BOEM concur with recommendation 3. BSEE and BOEM, in coordination with the Department, will utilize the DHS and DOI implementation of the Continuous Diagnostics and Monitoring (CDM) Dashboard and will augment it to incorporate organizational needs.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

NPS concurs with recommendation 3. NPS, in coordination with the Department, will utilize the DHS and DOI implementation of the Continuous Diagnostics and Monitoring (CDM) Dashboard and will augment it to incorporate organizational needs.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

USGS concurs with recommendation 3. USGS, in coordination with the Department, will utilize the DHS and DOI implementation of the Continuous Diagnostics and Monitoring (CDM) Dashboard and will augment it to incorporate organizational needs.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

Recommendations 4: FWS concurs with recommendation 4. The FWS will revise the bureau standard operating procedure (SOP) to enhance oversight of the [redacted] The SOP [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

Recommendation 5: FWS concurs with recommendation 5. The FWS will revise [redacted]
Responsible Official(s): ACIO
Target Completion Date: 6/30/2018

Recommendation 6: SOL concurs with recommendation 6. SOL will improve its compliance oversight with POA&M processes through its support partnership with the OCIO.
Responsible Official(s): ACIO - Tim Wight
Target Completion Date: 12/31/2018

Recommendation 7: BLM concurs with recommendation 7. BLM will create or update procedures to incorporate more detailed information and tracking of POA&Ms within CSAM.
Responsible Official(s): ACIO
Target Completion Date: 6/30/2018

Recommendations 8 and 9: BSEE and BOEM concur with recommendation 8 and 9. BSEE and BOEM will continue to implement and monitor their June 28, 2017, Information System Continuous Monitoring (ISCM) Strategy and periodically assess its effectiveness.
Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

Recommendation 10: OST concurs with recommendation 10. OST will ensure that a process/procedure is developed to add [redacted]
Responsible Official(s): ACIO
Target Completion Date: 6/30/2018

OST management stated the following: “Although we concur with the Notification of Finding, we wanted to explain below that we are working to update the form and policy based on discussions that occurred during the audit.” [redacted] We are in the process, under a POA&M, of updating the [redacted] and this section will be updated as part of that artifact update [redacted]

Recommendations 11 - 16:

BLM concurs with recommendation 11. BLM will implement [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

BLM concurs with recommendation 12. BLM will conduct a feasibility analysis and issue a report to [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

BLM concurs with recommendation 13. BLM will implement a process to perform [redacted] requirements for the [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

BLM concurs with recommendation 14. BLM will implement methods to [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

BLM concurs with recommendation 15. BLM will enhance [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

BLM concurs with recommendation 16. BLM will create a procedure and implement a process [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

BLM is conducting a review of [redacted] BLM is also consolidating [redacted] to minimize [redacted] in existence, allowing better management and audit capabilities of access to these [redacted] Limiting the duration that [redacted]

BLM management stated: "We will work with [redacted] and explore the options based [redacted] Once the process has been fully defined, policy will be issued. Any repercussions for not submitting an appropriate ticket is a Human Resources function and will be at their discretion."

"Per DOI security control standards requiring accounts be disabled after 45 days of inactivity, [redacted] sends an email notification to the listed manager/supervisor informing them of the account status and reminding them to submit the appropriate ticket."

Recommendation 17:

OST concurs with recommendation 17. OST has scheduled software and hardware updates for the [redacted] OST will implement a standard operating procedure to review [redacted]

Responsible Official(s): ACIO
Target Completion Date: 03/30/2018

OST management noted [redacted] will receive a software update to the most current version as well as a hardware update to a more robust computer. In conjunction, a standard operation procedure is being developed that details the [redacted] responding to any errors or violations and establishing a schedule for [redacted] to be conducted and documented at a minimum of semi-annually. Upon further inquiry, these proposed corrective actions were rescheduled to be completed March 31, 2018.

Recommendation 18: BOR concurs with recommendation 18. BOR will develop or update procedure documentation that will guide their [redacted]

Responsible Official(s): ACIO
Target Completion Date: 12/31/2018

Recommendations 19 and 20:
BLM concurs with recommendation 19. BLM will update the [redacted] to document how [redacted]

Responsible Official(s): ACIO
Target Completion Date: 6/30/2018

Response: BLM concurs with recommendation 20. BLM will implement procedures to ensure that i) [redacted] monitoring and reviews are consistently performed and ii) evidence of [redacted] is retained for at least one year.
Responsible Official(s): ACIO
Target Completion Date: 6/30/2018

BLM management noted the [redacted] are reviewed by the [redacted] and documented monthly. The logs are then posted to the [redacted]

The [redacted] also receives [redacted]. The card reader records all successful and failed attempts to gain access to the [redacted] The logs are reviewed when received, then [redacted] Although these logs are reviewed, [redacted] A step has been added to the process to for reviewing the reports [redacted]

[redacted] implementation statement for PE 6 will be updated to reflect the review processes.

Appendix I – Summary of Cybersecurity Framework Security Function Areas

The following table summarizes the Cybersecurity Framework Security Function areas in which control deficiencies were identified. It should not be used to infer program area compliance in general, and does not correlate to the overall program area assessments provided in Appendix V or responses provided for the FY2017 CyberScope Responses.

The Identify function area consists of risk management. The Protect function area consists of configuration management, identity and access management, and security training. The Detect function area consists of information system continuous monitoring. The Respond function area consists of incident response, and the Recover function area consists of contingency planning.

Functions	BIA	BLM	BOR	BSEE	BOEM	FWS	IBC	NPS	OIG	ONRR	OS	OSM	OST	SOL	USGS
Identify				**X**	**X**	**X**		**X**						**X**	**X**
Protect		**X**	**X**										**X**		
Detect				**X**	**X**										
Respond															
Recover															

Legend:
X – Weakness identified in Cybersecurity function

Appendix II – Listing of Acronyms

Acronym	Definition
A&A	Assessment & Authorizations
AC	Access Control
AO	Authorizing Official
ATO	Authority/Authorization to Operate
AU	Audit and Accountability
BCISO	Bureau Chief Information Security Officer
BCP	Business Continuity Plan
BIA	Bureau of Indian Affairs
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
CA	Security Assessment and Authorization
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspector General for Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CS	Contractor System
CSAM	Cyber Security Assessment and Management
CVE	Common Vulnerability and Exposures
DHS	Department of Homeland Security

Acronym	**Definition**
DOI	United States Department of the Interior
DRP	Disaster Recovery Plan
FCD	Federal Continuity Directive
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FPPS	Federal Personnel Payroll System
FTP	File Transfer Protocol
FWS	US Fish and Wildlife Service
FY	Fiscal Year
GSS	General Support System
HQ	Headquarters
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IA	Information Assurance
IAM	Identity and Access Management
IAPATRM	Information Assurance Policy, Security Architecture, Security Training and Risk Management
IG	Inspector General
IP	Internet Protocol
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
LAN	Local Area Network
MS	Microsoft
NFR	Notice of Findings and Recommendations

Acronym	**Definition**
NIST	National Institute of Standards and Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OHTA	Office of Historic Trust Accounting
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONRR	Office of Natural Resources Revenue
OS	Office of the Secretary
OS	Operating System
OSMRE	Office of Surface Mining Reclamation and Enforcement
OST	Office of the Special Trustee for American Indians
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestones
PUB	Publication
PY	Prior Year
RA	Risk Assessment
REV	Revision
RFQ	Request for Quotation
RM	Risk Management
SA	System and Services Acquisition
SC	System and Communication Protection
SCAP	Security Content Automation Protocol
SI	System and Information Integrity
SIEM	Security Information and Event Management

Acronym	**Definition**
SOL	Office of the Solicitor
SP	Special Publication
SSP	System Security Plan
ST	Security and Awareness Training
STIG	Security Technical Implementation Guide
TLS	Transport Layer Security
US	United States
US-CERT	United States Computer Emergency Readiness Team
USC	United States Code
USGS	United States Geological Survey

Appendix III – Prior Year Recommendation Status

Below is a summary table of the FY16 FISMA report recommendations and the status as of 9/30/2017.

Table 1. FY2016 FISMA Report Recommendations and Status as of 9/30/2017.
13 of 21 Recommendations are Open

Description	Status
1. Ensure OS and OCIO define and document roles, responsibilities and procedures for government oversight, monitoring and reporting of contractor provided systems and services to ensure contractors are performing, monitoring and reporting required security controls in accordance with contractual requirements.	Open. Target completion date of 12/31/2018.
2. BIA enforce existing processes to ensure IT [redacted] are implemented in accordance with the Department of the Interior, Security Control Standard for [redacted] and Develop a solution for the web server source code utilizing SSLv3 that would allow the upgrade to [redacted]	Closed. 7/3/2017
3. BLM complete the implementation of the [redacted] that will allow BLM to effectively [redacted] connected to the network.	Closed. 3/30/2017
4. BOR test and deploy the latest appropriate [redacted] ensure approved configuration baselines are applied.	Open. Target completion date 2/2/2018.
5. BSEE implement a follow up process to address those systems that fail initial [redacted] to ensure all devices are [redacted] in a timely manner. Systems that require extensive testing prior to patching that could affect the due dates [redacted] should be identified and addressed appropriately by management.	Closed. 6/15/2017
6. FWS enhance oversight and compliance to ensure all relevant and appropriate [redacted] in order to effectively implement [redacted] as required. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.	Open. Target completion date 12/31/2017.
7. NPS augment the existing testing and [redacted] to ensure effective coordination efforts between separate entities occur, allowing [redacted] to be remediated timely in accordance with the Department of the Interior, Security Control Standard fo[redacted]	Open. Target completion date of 10/1/2017.
8. OIG ensure [redacted] in accordance with the Department of the Interior, Security Control Standard [redacted] and maintain POA&Ms for [redacted] requiring additional time for implementation.	Closed. 6/21/2017
9. USGS ensure the proper authentication is used in performing credentialed vulnerability scanning on all moderate and high-impact networked devices within [redacted]	Open. Target completion date 12/31/2018.
10. BIA formally document and implement a process for the review of [redacted], retain the results of the review and enhance the account management process to ensure that all network [redacted] are appropriately disabled after 90 days or at the time of user [redacted]	Closed. 3/30/2017

11. USGS identify, document, and implement a solution to [redacted] before connecting to the network. Define and implement processes to ensure that the PIV is enabled for at least 85% of [redacted]. USGS and [redacted] should enhance existing procedures to ensure [redacted] are reviewed at least annually.	Open. Target completion date 5/1/2018 and 1/30/2020.
12. OS and OCIO define and document how ISCM activities that will integrate with organizational risk tolerance, the threat environment, business requirements, and shared with individuals with significant security responsibilities and used to make risk-based decisions. Identify, define and document the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program and control ongoing risk, and define and document processes for collecting and considering lessons learned to improve ISCM processes and disseminate to its Bureaus and Offices. Define and document how it will use automation to produce an accurate [redacted] of the [redacted] on its network and the [redacted] of its software.	Open. Target completion date 12/31/2018.
13. BSEE and NPS fully define and document procedures to integrate ISCM activities with risk tolerance, the threat environment, and business requirements. Document procedures to routinely aggregate and summarize operational ISCM data to appropriate levels for regular reporting to individuals with significant responsibilities. Document qualitative and quantitative performance measures to assess the effectiveness of bureau ISCM program and process for collecting lessons learned to improve ISCM processes.	Open. Target completion date of 10/1/2017
14. NPS validate proper implementation of [redacted] on all servers on the [redacted]	Closed. 3/30/2017
15. Formally approve and communicate throughout the Department updated incident response policies and procedures.	Closed. 9/18/2017
16. Define qualitative and quantitative performance measures that will be used to assess the effectiveness and maturity of its incident response program.	Open. Target completion date of 6/1/2018
17. Continue to define and implement technology tools, such as a [redacted] that advance incident detection and response capabilities.	Open. Target completion date of 8/31/2018
18. Define how to utilize technology to develop and maintain a [redacted] traffic for users and systems.	Open. Target completion date of 12/24/2018

19. BLM and USGS update their respectively contingency plans, BLM [redacted] contingency plan and the USGS [redacted] contingency plans in accordance with NIST requirements.	Closed. 3/30/2017
20. FWS review and update the FWS COOP Plan. The COOP should be updated in accordance with [redacted] equirements not addressed by the DOI COOP plan. FWS develop a BCP. The BCP should focus on sustaining an organization's mission business processes during and after a disruption.	Open. Target completion date of 12/31/2017
21. OSM and OST test their respective contingency plans, [redacted] Contingency Plan and the OST Contingency Plan in accordance with NIST requirements. The test documentation should include methodology, procedures, results, and lessons learned. Where necessary, the OSM and OST contingency plans should be updated based on the results of the contingency plan test.	Open. Target completion dates of 6/30/2017 and 12/31/2017.

Appendix IV – NIST SP 800-53 Security Controls Cross-Referenced the Cybersecurity Framework Function Areas.

The table below represents the Cybersecurity Framework function areas of Identify, Detect, Protect, Respond, and Recover with the associated NIST SP 800-53 security controls that KPMG considered during the performance audit.

Cybersecurity Framework Identify Function Area: Risk Management	
NIST SP 800-53: CA-3	System Interconnections
NIST SP 800-53: CA-5	Plan of Action and Milestones
NIST SP 800-53: CA-7	Continuous Monitoring
NIST SP 800-53: CM-4	Security Impact Analysis
NIST SP 800-53: CM-8	Information System Component Inventory
NIST SP 800-53: CM-10	Software Usage Restrictions
NIST SP 800-53: RA-1	Risk Assessment Policy and Procedures
NIST SP 800-53: RA-2	Security Categorization
NIST SP 800-53: PL-2	System Security Plan
NIST SP 800-53: PL-8	Information Security Architecture
NIST SP 800-53: PM-5	Information System Inventory
NIST SP 800-53: PM-7	Enterprise Architecture
NIST SP 800-53: PM-8	Critical Infrastructure Plan
NIST SP 800-53: PM-9	Risk Management Strategy
NIST SP 800-53: PM-11	Mission/Business Process Definition
NIST SP 800-53: SA-3	System Development Life Cycle
NIST SP 800-53: SA-4	Acquisition Process
NIST SP 800-53: SA-8	Security Engineering Principles
Cybersecurity Framework Protect Function Area: Configuration Management	
NIST SP 800-53: CM-1	Configuration Management Policy and Procedures
NIST SP 800-53: CM-2	Baseline Configuration
NIST SP 800-53: CM-3	Configuration Change Control
NIST SP 800-53: CM-6	Configuration Settings
NIST SP 800-53: CM-7	Least Functionality
NIST SP 800-53: CM-8	Information System Component Inventory
NIST SP 800-53: CM-9	Configuration Management Plan
NIST SP 800-53: SI-2	Flaw Remediation
Cybersecurity Framework Protect Function Area: Identity and Access Management	
NIST SP 800-53: AC-1	Access Control Policy and Procedures
NIST SP 800-53: AC-2	Account Management
NIST SP 800-53: AC-8	System Use Notification
NIST SP 800-53: AC-17	Remote Access
NIST SP 800-53: IA-1	Identification and Authentication Policy and Procedures
NIST SP 800-53: SI-4	Information System Monitoring
NIST SP 800-53: PL-4	Rules of Behavior
NIST SP 800-53: PS-1	Personnel Security Policy and Procedures
NIST SP 800-53: PS-2	Position Risk Determination
NIST SP 800-53: PS-3	Personnel Screening
NIST SP 800-53: PS-6	Access Agreements
Cybersecurity Framework Protect Function Area: Security Training	
NIST SP 800-53: AT-1	Security Awareness and Training Policy and Procedures

NIST SP 800-53: AT-2	Security Awareness Training
NIST SP 800-53: AT-3	Role-Based Security Training
NIST SP 800-53: AT-4	Security Training Records
Cybersecurity Framework Detect Function Area: Information System Continuous Monitoring	
NIST SP 800-53: CA-1	Security Assessment and Authorization Policy and Procedures
NIST SP 800-53: CA-2	Security Assessments
NIST SP 800-53: CA-6	Security Authorization
NIST SP 800-53: CA-7	Continuous Monitoring
Cybersecurity Framework Respond Function Area: Incident Response	
NIST SP 800-53: IR-1	Incident Response Policy and Procedures
NIST SP 800-53: IR-4	Incident Handling
NIST SP 800-53: IR-6	Incident Reporting
Cybersecurity Framework Recover Function Area: Contingency Planning	
NIST SP 800-53: CP-1	Contingency Planning Policy and Procedures
NIST SP 800-53: CP-2	Contingency Plan
NIST SP 800-53: CP-3	Contingency Pan Training
NIST SP 800-53: CP-4	Contingency Plan Testing
NIST SP 800-53: CP-6	Alternate Storage Site
NIST SP 800-53: CP-7	Alternate Processing Site
NIST SP 800-53: CP-8	Telecommunications Services
NIST SP 800-53: CP-9	Information System Backup
NIST SP 800-53: IR-4	Incident Handling

Appendix V – Responses to the Department of Homeland Security's FISMA 2017 Questions for Inspectors General

The information included represents the Department of the Interior (DOI) responses to Department of Homeland Security's (DHS) FISMA 2017 questions for Inspectors General.

The information included in this appendix represents KPMG's responses on behalf of the Department of the Interior (DOI) Inspector General (IG) to the Department of Homeland Security's (DHS) FISMA 2017 questions for the annual independent evaluation of DOI's security program.

DHS provides a general description of the five IG Assessment Maturity Levels, as shown in Table 1:

Table 1: IG Assessment Maturity Levels

Maturity Level	FY 2017 IG FISMA Metric Domains
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

For each FISMA question assessed at maturity Level 1, 2, or 3, we explained in each "Comment" area why maturity Level 4 was not obtained. Given the changes to the FY 2017 IG FISMA Reporting Metrics, a year-on-year comparison for FISMA compliance may not be feasible.

Function 0 is the overall summary for the FISMA Performance Audit for DOI. Functions 1–5 follow the 5 Cybersecurity Functions.

Function 0: Consistently Implemented (Level 3)

0.1 Please provide an overall IG self-assessment rating: Based on results of testing, the maturity level was assessed as Consistently Implemented (Level 3), which is not effective.

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

Comments:

A Performance Audit was conducted over the information security program and practices of the Department of the Interior (DOI) to determine the effectiveness of such programs and practice for the fiscal year ending September 30, 2017. The scope of the audit included the following Bureaus and Offices, Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Ocean and Energy Management (BOEM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and

Wildlife Service (FWS), Interior Business Center (IBC), National Park Service (NPS), Office of the Inspector General (OIG), Office of Natural Resources Revenue (ONRR), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), Office of the Special Trustee for American Indians (OST), Office of the Solicitor (SOL), and U.S. Geological Survey (USGS). DOI had 125 operational unclassified information systems and 15 information systems were randomly selected for the audit.

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, DOI established and maintained its information security program and practices in the five cybersecurity functions, Identify, Protect, Detect, Respond, and Recover. However, the program was not fully effective, as deficiencies were identified in each cybersecurity function area. Deficiencies were noted in the FISMA domain areas of risk management, configuration management, information security continuous monitoring, incident response, and contingency planning metric domains. Consistent with the Fiscal Year (FY) 2017 OIG FISMA metric rating instructions, ratings throughout the seven FISMA domains were identified by a simple majority, where the most frequent level across the FISMA metrics served as the domain rating. KPMG assessed the cybersecurity function areas of Identify, Protect, Detect and Recover as Consistently Implemented (Level 3) and the Respond function as Defined (Level 2). Overall, DOI was assessed at Consistently Implemented (Level 3).

Function 1: Identify – Risk Management

1 Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 –4)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization maintains a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third party systems), and system interconnections.

Comments: DOI maintains an inventory of its information systems in the [redacted] nd [redacted] is used to assess, document, manage, and report on the status of information technology security risk and control assessments, and implementation of Federal and the DOI Security Control Standards. This is the highest available maturity level for this metric.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2)?

Maturity Level: **Managed and Measured (Level 4)** - The organization ensures that the hardware assets connected to the network are subject to the monitoring processes defined within the organization's ISCM strategy.

Comments: Through automated mechanisms, 10 of 15 Bureaus and Offices, [redacted], [redacted] monitor hardware assets connect to the network.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Maturity Level: **Defined (Level 2)** - The organization has defined, but not consistently implemented, a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting.

Comments: DOI has not implemented a consistent process to ensure that inventory of software assets connected to the network is current. According to audit report No: 2016-ITA-062, *The U.S. Department of the Interior Office of Inspector General Federal Information Security Modernization Act of 2014, Fiscal Year 2016 Performance Audit*, dated February 10, 2017 recommendation remains open.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?

Maturity Level: **Consistently Implemented (Level 3)** - Information on the organization's defined importance/priority levels for its missions, business functions, and information is consistently used and integrated with other information security areas to guide risk management activities and investments in accordance with applicable requirements and guidance.

Comments: 13 of 15 Bureaus and Office, [redacted] have consistently defined their mission and business functions in their respective risk management policies and procedures. [redacted] have not fully implemented its risk management policies and procedures at the enterprise, business process, and information system levels. This is the highest available maturity level for this metric.

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Maturity Level: **Consistently Implemented (Level 3**) - The organization consistently implements its risk management policies, procedures, and strategy at the enterprise, business process and information system levels. The organization uses its risk profile to facilitate a determination on the aggregate level and types of risk that management is willing to assume. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of risk management processes and activities to update the program.

Comments: Nine of 15 Bureaus and offices, [redacted] have not defined, monitored, or reported qualitative and quantitative performance measures on the effectiveness of the risk management program. Also, [redacted] have not fully implemented its risk management policies and procedures at the enterprise, business process, and information system levels.

DOI can improve and increase its maturity level by defining, monitoring and reporting qualitative and quantitative performance measures on the effectiveness of the risk management program.

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization 's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Maturity Level: **Consistently Implemented (Level 3**) - The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. Security architecture reviews are consistently performed for new/acquired hardware/software prior to introducing systems into the organization's development environment.

Comments: 10 of 15 Bureaus and Offices, [redacted] have implemented a security architecture at the bureau and information system levels. However; [redacted] have not developed or reviewed an information system architecture. This is the highest available maturity level for this metric.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer,

and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Maturity Level: **Consistently Implemented (Level 3) -** Roles and responsibilities of stakeholders involved in risk management have been defined and communicated across the organization. Stakeholders have adequate resources (people, processes, and technology) to effectively implement risk management activities.

Comments: DOI has defined roles and responsibilities of risk management stakeholders such as Chief Information Officer, Chief Information Security Officer, System Owner, and Authorizing Official.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization consistently implements POA&Ms, in accordance with the organization's policies and procedures, to effectively mitigate security weaknesses.

Comments: 13 of 15 Bureaus and Offices, [redacted] have implemented POA&Ms in accordance with the DOI POA&M Standards. [redacted] are not consistently reviewing or updating POA&Ms on a quarterly basis in accordance with DOI security policy. Also, DOI does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information, as needed, to ensure that its risks posture is maintained.

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing:
(i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
(ii) internal and external asset vulnerabilities, including through vulnerability scanning,
(iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
(iv) selecting and implementing security controls to mitigate system-level risks (NIST 800-37; NIST 800-39; NIST 800-53: PL-2, RA-1; NIST 800-30; CSF: ID.RA-1 – 6)

Maturity Level: **Consistently Implemented (Level 3**) **-** System risk assessments are performed and appropriate security controls are implemented on a consistent basis. The organization utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities.

Comments: DOI has performed system risk assessments in accordance the DOI Security Control Standards and identified the appropriate security controls to be implemented at the information system level.

DOI can improve and increase its maturity level by consistently monitoring the effectiveness of risk responses to ensure that enterprise-wide risk tolerance is maintained at an appropriate level.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization ensures that information about risks is communicated in a timely and consistent manner to all internal and external stakeholders with a need-to-know. Furthermore, the organization actively shares information with partners to ensure that accurate, current information is being distributed and consumed.

Comments: DOI has consistently communicated risks in a timely manner to stakeholders such as Associate Chief Information Officers, Chief Information Security Officers, System Owners, and System

Administrators. Communication methods include email and various security working groups that meet periodically to discuss potential risks and threats to the department. In connection with the Department of Homeland Security (DHS) Continuous Diagnostic and Mitigation Program, DOI is developing the framework and roles and responsibilities for reporting, including dashboards that facilitate a portfolio view of risk across the organization.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007-004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8).

Maturity Level: **Ad Hoc (Level 1) -** The organization has not defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for contractor systems and services include appropriate clauses to monitor risks related to such systems and services. Further, the organization has not defined its processes for ensuring appropriate information security oversight of contractor provided systems and services.

Comments: DOI has not defined processes and procedures for monitoring contractor-operated systems. According to audit report No: 2016-ITA-062, *The U.S. Department of the Interior Office of Inspector General Federal Information Security Modernization Act of 2014, Fiscal Year 2016 Performance Audit*, dated February 10, 2017 recommendation remains open. Also, DOI does not use qualitative and quantitative performance metrics to measure, report on, and monitor information security performance of contractor-operated systems and services.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Maturity Level: **Consistently Implemented (Level 3**) - The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise wide view of risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of risk information are integrated into the solution.

Comments: 9 of 15 Bureaus and Office, [redacted] have implemented a bureau-level solution that provides a centralized view of risk and management dashboards. [redacted] did not define and implement a solution that provides a centralized view of risks across the organization, including risk control and remediation activities, and management dashboards. Also, DOI does not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to DOI systems and data.

13.1 Please provide the assessed maturity level for the agency's Identify – Risk Management function.

Comments: **Consistently Implemented (Level 3).** Nine of 12 risk management metrics were assessed at level 3.

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

Comments: No additional testing was performed beyond the above metrics. The risk management program is not effective.

Function 2A: Protect – Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800- 53: CM-1; SP 800-128: Section 2.4)?

Maturity Level: **Consistently Implemented (Level 3)** - Stakeholders have adequate resources (people, processes, and technology) to consistently implement information system configuration management activities.

Comments: 13 of 15 Bureaus and Office, [redacted], [redacted] have resources to adequately implement the information system configuration management activities. [redacted] have not fully defined roles and responsibilities in their respective configuration management procedures at the information system level. Also, Staff are not assigned responsibilities for developing and maintaining metrics on the effectiveness of information system configuration management activities. DOI is not consistently collecting, monitoring, analyzing, and updating qualitative and quantitative performance measures across the organization and is reporting data on the effectiveness of the organization's information system configuration management program to the Chief Information Security Officer.

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800-128: Section 2.3.2; NIST 800-53: CM-9)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented an organization-wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.

Comments: 12 of 15 Bureaus and Offices, [redacted], [redacted] have not defined, monitored, or reported qualitative and quantitative performance measures on the effectiveness of the configuration management program. Also, DOI does not monitor, analyze, and report to stakeholders' qualitative and quantitative performance measures on the effectiveness of its configuration management plan.

DOI can improve and increase its maturity level by defining, monitoring, and reporting qualitative and quantitative performance measures on the effectiveness of the configuration management program.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST 800-128: 2.2.1)

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures.

Comments: 14 of 15 Bureaus and Offices, [redacted], [redacted] have implemented policies and procedures for managing the configuration of its information system. [redacted] did not maintain [redacted]

DOI has not required the Bureaus and Offices to monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its configuration management policies and procedures.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.

Comments: 12 of 15 Bureau and Offices, [redacted], [redacted] have implemented configuration management change control in accordance with Department Security Control Standards. However, [redacted] did not record or maintain [redacted] in accordance with DOI Security Control Standards. [redacted] did not document procedures for maintaining a [redacted] Also, DOI has not fully implemented processes and automated technology to [redacted]

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Maturity Level: **Consistently Implemented (Level 3)** – The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes [redacted] against all systems on the network to assess and manage both code-based and configuration-based vulnerabilities.

Comments: 14 of 15 Bureaus and Offices, [redacted], [redacted] have developed, documented, and disseminated its policies and procedures and maintained configuration build guides. However, [redacted] was unable to provide configuration baseline security standards for its information system for evaluation. DOI has not implemented automation to help maintain a [redacted] for all information system components connected to the network.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

Maturity Level: **Managed and Measurable (Level 4) -** The organization centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.

Comments: DOI is managing its flaw remediation process and utilizes automated patch management and software update tools for operating system. The technology is [redacted]

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization has consistently implemented its TIC approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate, and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.

Comments: DOI has consistently implemented TIC approved connections and manages the connections effectively. This is the highest available maturity level for this metric.

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM-2, CM-3)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its change control policies, procedures, and processes, including explicitly consideration of security impacts prior to implementing changes.

Comments: 13 of 15 Bureaus and Offices, [redacted], [redacted] have implemented change control policies and procedures. However, ONRR change control policies and procedures do not consider security implications prior to implementing a change. [redacted] does not maintain documentation of system changes performed on the [redacted] Also, DOI does not define qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures data supporting the metric is obtained accurately, consistently, and in a reproducible format.

22 Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

Comments: No additional testing was performed beyond the above metrics. Seven of eight configuration management metrics were assessed at level 3. The configuration management program is not effective.

Function 2B: Protect – Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Maturity Level: **Consistently Implemented (Level 3) -** Stakeholders have adequate resources (people, processes, and technology) to effectively implement identity, credential, and access management activities.

Comments: 13 of 15 Bureaus and Offices [redacted] have implemented effective identity, credential, and access management activities, but have not developed, managed, or monitored metrics on the effectiveness of ICAM activities. [redacted] have implemented performance metrics to measure the effectiveness of the ICAM program.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Maturity Level: **Consistently Implemented (Level 3**) - The organization is consistently implementing its ICAM strategy and is on track to meet milestones?

Comments: DOI has implemented their ICAM strategy and is on track to meet milestones in order to meet its desired ICAM architecture.

DOI can improve and increase its maturity level by fully implementing its desired ICAM architecture and integrates its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 27 through 31) (NIST 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Maturity Level: **Managed and Measureable (Level 4) -** The organization uses automated mechanisms (e.g. machine-based, or user based enforcement), where appropriate, to manage the effective implementation of its policies and procedures. Examples of automated mechanisms include network segmentation based on the label/classification of information stored on the servers; automatic removal/disabling of temporary/emergency/inactive accounts, use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.

Comments: 13 of 15 Bureaus and Offices, [redacted] have implemented a process to manage the implementation of its policies and procedures. [redacted] in accordance with DOI Security Control Standards.

DOI can improve and increase its maturity level by implementing adaptive identification and authentication techniques to assess suspicious behavior and potential violations of its ICAM policies and procedures on a near-real time basis.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.

Comments: Eight of 15 Bureaus and Offices [redacted] have assigned risk designations and appropriately screened personnel prior to granting system access. Seven of 15 Bureaus and Offices, [redacted] employed automation to centrally document, track, and share risk designations and screening information.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800-53: AC-8, PL-4, and PS-6)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. The organization utilizes more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

Comments: DOI reviews and maintains access agreements such as rule of behavior for individuals prior to granting system access. This is the highest available maturity level for the metric.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Maturity Level: **Managed and Measureable (Level 4) -** All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

Comments: 12 of 15 Bureaus and Offices, [redacted] utilize strong authentication for authenticating non-privileged users to applicable information systems. [redacted] have not fully implemented strong authentication such as Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) cards for non-privileged users to applicable information systems.

DOI can improve and increase its maturity level by fully implementing an enterprise-wide single sign on solution and all information systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a nearly real-time basis.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Maturity Level: **Managed and Measurable (Level 4)**: All privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

Comments: 12 of 15 Bureaus and Offices, [redacted] have implemented strong authentication such as Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) cards to authenticate privileged users to applicable information systems [redacted] have not fully implemented strong authentication for privileged users to applicable information systems.

DOI can improve and increase its maturity level by fully implementing an enterprise-wide single sign on solution and all information systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a nearly real-time basis.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Maturity Level: **Managed and Measurable (Level 4) -** The organization employs automated mechanisms (e.g. machine-based, or user based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.

Comments: Nine of 15 Bureaus and Offices, [redacted] have effectively implemented procedures to support the management of privileged accounts for the removal and disabling of temporary and inactive accounts.

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC-17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Maturity Level: **Managed and Measurable (Level 4):** The organization ensures that end user devices have been appropriately configured prior to allow remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.

Comments: DOI has effectively implemented technology [redacted]

DOI can improve and increase its maturity level by [redacted]

32 Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Comments: No additional testing was performed beyond the above metrics. **Managed and Measurable (Level 4):** Five (5) of nine (9) IAM related metrics were assessed at Managed and Measurable (Level 4). The identity and access management program is effective.

Function 2C: Protect – Security Training

33 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST 800-53: AT-1; and NIST SP 800-50)?

Maturity Level: **Managed and Measureable (Level 4) -** The organization has assigned responsibility for monitoring and tracking the effectiveness of security awareness and training activities. Staff is consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

Comments: DOI is tracking and measuring the effectiveness of security awareness and training activities within its enterprise-wide learning management system, DOI Learn. The system contains over 1,200 instructor-led courses and over 4,000 online courses.

34 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

Maturity Level: **Managed and Measureable (Level 4) -** The organization has addressed all of its identified knowledge, skills, and abilities gaps. Skilled personnel have been hired and/or existing staff trained to develop and implement the appropriate metrics to measure the effectiveness of the organization's training program in closing identified skill gaps.

Comments: DOI has either addressed or is actively addressing knowledge, skill, or abilities gaps. Specifically, staff were hired to assist in policy development for the DOI ISCM program and related continuous diagnostic management activities.

DOI can improve and increase its maturity level by ensuring the personnel collectively possess a training level such that the department can demonstrate that security incidents resulting from personnel actions or inaction are being reduced over time.

35 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST 800-53: AT-1; NIST 800-50: Section 3))

Maturity Level: **Managed and Measureable (Level 4) -** The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

Comments: DOI monitors the effectiveness of its security awareness and training program. Performance is measured in the DOI Learn management system.

DOI can improve and increase its maturity level by ensuring the security awareness and training activities are integrated across other security-related domains. For example, common risks and control weaknesses, and other outputs of the department's risk management and continuous monitoring activities inform any updates that need to be made to the security awareness and training program.

36 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

Maturity Level: **Managed and Measureable (Level 4)** - The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

Comments: DOI monitors and analyzes security training performance measures over its security awareness and training program. Performance is captured in the DOI Learn management system.

DOI can improve and increase its maturity level by ensuring Bureaus and Offices on a near real-time basis, actively adapts its security awareness and training policies, procedures, and program to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.

37 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Maturity Level: **Consistently Implemented (Level 3)** - The organization ensures that all systems users complete the organization's security awareness training (or a comparable awareness training for contractors) prior to system access and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.

Comments: DOI ensures that information system users complete Federal Information System Security Awareness Plus training prior to system access and refresher training is required annually. Training records are maintained in the centralized DOI Learn management system. [redacted]

38 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization ensures individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records. Furthermore, the organization maintains specialized security training completion records.

Comments: DOI ensures that staff with significant security responsibilities such as Bureau Chief Information Security, Authorizing Official, and System Owner perform role-based security training at least annually. Training records are maintained in the centralized DOI Learn management system. [redacted]

39.1 Please provide the assessed maturity level for the agency's Protect – Configuration Management/Identity and Access Management/Security Training (Functions 2A- 2C).

Comments: For configuration management, seven of eight metrics were assessed at Consistently Implemented (Level 3). For identity and access management, five of nine metrics were assessed at Managed and Measurable (Level 4). For security training, four of six metrics were assessed at Managed and Measurable (Level 4). Overall, 13 of 23 metrics were assessed at Consistently Implemented (Level 3) and 10 of 23 were assessed at Managed and Measurable (Level 4).

39.2 Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

Comments: No additional testing was performed beyond the above metrics. Four of six security training metrics were assessed at Managed and Measurable (Level 4). The security training program is effective.

Function 3: Detect – ISCM

40 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization's ISCM strategy is consistently implemented at the organization/business process and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy.

Comments: 12 of 15 Bureaus and Offices, [redacted] have consistently implemented their respective ISCM strategies. However, [redacted] and [redacted] have not fully implemented their new ISCM program that was approved in June, 2017. [redacted] did not consistently report key information, such as monthly vulnerability assessment test results and quarterly POA&M reports, to the authorizing official in accordance with DOI Information Security Control Standards. Also, DOI does not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and data supporting metrics are obtained, accurately, and consistently.

41 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7). (Note: The overall maturity level should take into consideration the maturity of question 43)

Maturity Level: **Consistently Implemented (Level 3) -** The organization's ISCM policies and procedures have been consistently implemented for the specified areas. The organization also consistently captures lessons learned to make improvements to the ISCM policies and procedures.

Comments: 12 of 15 Bureaus and Offices, [redacted] have consistently implemented their respective ISCM strategies. However, [redacted] [redacted] have not fully implemented their new ISCM program that was approved in June, 2017. [redacted] did not consistently report key information, such as monthly vulnerability assessment test results and quarterly POA&M reports, to the authorizing official in accordance with DOI Information Security Control Standards. Also, DOI has not defined qualitative and quantitative performance metrics to measure the effectiveness of the ISCM policies and procedures.

42 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?

Maturity Level: **Consistently Implemented (Level 3) -** Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Comments: 12 of 15 Bureaus and Offices, [redacted], [redacted] have defined roles and responsibilities over their respective ISCM programs. [redacted] and [redacted] have not fully implemented its ISCM program and [redacted] has not fully defined its roles and responsibilities for ISCM stakeholders. Also, DOI has not defined qualitative and quantitative performance metrics to measure the effectiveness of the ISCM policies and procedures.

43 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Maturity Level: **Managed and Measureable (Level 4)** – The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorization of information systems.

Comments: Information system owners and authorizing officials review key assessment and authorization documentation such as results of annual control assessments and plan of action and milestones.

DOI can improve and increase its maturity level by ensuring the ISCM program achieves cost-effective IT security objectives and goals and influences decision-making that is based on cost, risk, and mission impact.

44 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Maturity Level: **Ad Hoc (Level 1) -** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. Further, the organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions.

Comments: DOI has not formally defined qualitative and quantitative performance metrics to measure effectiveness of the ISCM policies and procedures.

45.1 Please provide the assessed maturity level for the agency's Detect – ISCM Function.

Comments: Three of five ISCM metrics were assessed at Consistently Implemented (Level 3).

45.2 Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

Comments: No additional testing was performed beyond the above metrics. The ISCM program is not effective.

Function 4: Respond – Incident Response

46 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - 52)

Maturity Level: **Defined (Level 2)** - The organization's incident response policies, procedures, plans, and strategies have been defined and communicated. In addition, the organization has established and communicated an enterprise level incident response plan.

Comments: On August 28, 2017, DOI approved and disseminated its updated DOI Enterprise Computer Security Incident Response Plan to all its Bureaus and Offices. DOI can improve and increase its maturity level by fully implementing its IR plan.

47 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Maturity Level: **Defined (Level 2)** – The organization has defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority and dependencies. In addition, the organization has designated a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities.

Comments: On August 28, 2017; DOI approved and disseminated its updated DOI Enterprise Computer Security Incident Response Plan to all its Bureaus and Offices. DOI can improve and increase its maturity level by fully implementing its IR plan.

48 How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; US- CERT Incident Response Guidelines)?

Maturity Level: **Defined (Level 2)** - The organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.

Comments: On August 28, 2017; DOI approved and disseminated its updated DOI Enterprise Computer Security Incident Response Plan to all its Bureaus and Offices. DOI can improve and increase its maturity level by fully implementing its IR plan.

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

Maturity Level: **Defined (Level 2)** - The organization has developed containment strategies for each major incident type. In developing its strategies, the organization takes into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution. In addition, the organization has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.

Comments: On August 28, 2017; DOI approved and disseminated its updated DOI Enterprise Computer Security Incident Response Plan to all its Bureaus and Offices. DOI can improve and increase its maturity level by fully implementing its IR plan.

50 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Maturity Level: **Managed and Measured (Level 4)** - Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

Comments: The DOI Computer Incident Response Center (DOI-CIRC) measures and manages timely reporting of incident information to DOI officials such as the Chief Information Officer, Chief Information Security Officer and external organizations such as Department of Homeland Security (DHS), US-CERT, and law enforcement. This is the highest available maturity level for this metric.

51 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently utilizes on-site, technical assistance/surge capabilities offered by DHS or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization is utilizing [redacted] for intrusion detection/prevention capabilities for traffic entering and leaving its network.

Comments: When appropriate, DOI has the capability to leverage the services of DHS and other organizations for additional incident response capability. DOI has implemented [redacted] which detects and alerts to known or suspected cyber threats using Intrusion Detection System (IDS) technology. This is the highest available maturity rating for this metric.

52 To what degree does the organization utilize the following technology to support its incident response program?
- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)

Maturity Level: **Consistently Implemented (Level 3)** - The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

Comments: DOI has implemented many of the above tools and technology. Tools and technology such as firewalls, malware detection, data loss prevention technology, and endpoint and server security tools are implemented. The Department updated its incident tracking and reporting tool in order to effectively report incident information according to US-CERT reporting requirements. Also, DOI is currently implementing security information and event management (SIEM) tools at the Office of the Secretary.

53.1 Please provide the assessed maturity level for the agency's Respond – Incident Response function.
Comments: **Defined (Level 2).** Four of seven metrics were assessed at Defined (Level 2).

53.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

Comments: No additional testing was performed beyond the above metrics. The incident response program is not effective.

Function 5: Recover – Contingency Planning

54 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Maturity Level: **Consistently Implemented (Level 3)** - Roles and responsibilities of stakeholders involved in information system contingency planning have been fully defined and communicated across the organization. In addition, the organization has established appropriate teams that are ready to implement its information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes, and technology) to effectively implement system contingency planning activities.

Comments: DOI defined roles and responsibilities of stakeholders in the information system contingency planning program. However, DOI has not assigned responsibility for monitoring and tracking the effectiveness of information systems contingency planning activities. Staff is not consistently collecting, monitoring, and analyzing quantitative and qualitative performance measures on the effectiveness of the contingency planning program activities, including validation of IT system or system component to support essential functions.

55 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 56-60) (NIST SP 800-34; NIST SP 800-161).

Maturity Level: **Consistently Implemented (Level 3)** - The organization consistently implements its defined information system contingency planning policies, procedures, and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program.

Comments: 14 of 15 Bureaus and Offices, [redacted] have implemented information system contingency planning policies and procedures in accordance with DOI Security Control Standards. Lessons learned are communicated in the results of annual contingency plan tests and exercises. [redacted] conducted a contingency plan exercise in fiscal year 2017; however, the exercise did not include a functional test in accordance with the DOI Security Control Standards.

DOI can improve and increase its maturity level by ensuring Bureaus and Offices understands and manages its information and communication technology (ITC) supply chain risks related to contingency planning activities. As appropriate, Bureau and Offices: integrates supply chain concerns into its contingency planning policies, procedures, defines and implements a contingency plan for its ICT supply chain infrastructure, applies appropriate ICT supply chain controls to alternate storage and processing sites, considers alternate telecommunication service providers for its ICT supply chain infrastructure and to support critical information systems.

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800-34, Rev. 1, 3.2, FIPS 199, FCD-1, OMB M-17-09)?

Maturity Level: **Consistently Implemented (Level 3)** - The organization incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA and include: characterization of all system components, determination of missions/business processes and recovery criticality, identification of resource requirements, and identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high-value assets.

Comments: When appropriate, DOI conducts business impact analysis in support of contingency planning activities. This is the highest available maturity level for this metric.

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Maturity Level: **Consistently Implemented (Level 3) -** Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.

Comments: DOI consistently implemented information system contingency plans in accordance with DOI Security Control Standards. DOI has not defined performance metrics to measure the effectiveness of the contingency plans with information on the effectiveness of related plans such as Bureau or Office continuity of operations plan or disaster recovery plan to deliver situational awareness.

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

Maturity Level: **Consistently Implemented (Level 3) -** Processes for information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.

Comments: 14 of 15 Bureaus and Offices, [redacted] have implemented contingency plan testing and exercises. [redacted] conducted a contingency plan exercise in fiscal year 2017; however, the exercise did not include a functional test in accordance with the DOI Security Control Standards. Also, DOI has not implemented automated mechanisms to thoroughly and effectively test system contingency plans.

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Maturity Level: **Consistently Implemented (Level 3) -** The organization consistently implements its processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID,[5] as appropriate. Alternate processing and storage sites are chosen based upon risk assessments, which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. In addition, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, backups of information at the user- and system-levels are consistently performed and the confidentiality, integrity, and availability of this information is maintained.

Comments: DOI has consistently implemented information system backup and storage. This is the highest available maturity level for this metric.

[5] Redundant Array of Independent Disks (RAID) is a common practice of storing the same data in different places on many hard disks to protect the data in the event of a disk failure.

60 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST 800-53: CP-2, IR-4)?

Maturity Level: **Consistently Implemented (Level 3)** - Information on the planning and performance of recovery activities is consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk based decisions.

Comments: 11 of 15 Bureaus and Offices, [redacted], [redacted] have not collected data to support metrics on the effectiveness of recovery activities and communicated to relevant stakeholders. [redacted] maintains performance metrics to measure the effectiveness of their respective recovery activities.

61.1 Please provide the assessed maturity level for the agency's Recover – Contingency Planning function. Comments: Consistently Implemented (Level 3). Seven of seven metrics were assessed at Consistently Implemented (Level 3).

61.2 Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

Comments: No additional testing was performed beyond the above metrics. The contingency program is not effective.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doioig.gov

By Phone:

	24-Hour Toll Free:	800-424-5081
	Washington Metro Area:	202-208-5300

By Fax: 703-487-5402

By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240