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 2018

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

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

MAR 13 2019

Memorandum

To: William E. Vajda
Chief Information Officer

From: 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 2018
Report No. 2018-ITA-043

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) 2018. 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 2018 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. OIG does 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-19-02, "Fiscal Year 2018–2019 Guidance on Federal Information Security and Privacy Management Requirements," dated October 25, 2018.

KPMG reviewed information security practices, policies, and procedures at the DOI Office of the Chief Information Officer and the following 11 DOI bureaus and offices:

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

- Office of Inspector General
- Office of the Secretary
- Office of Surface Mining Reclamation and Enforcement
- Office of the Special Trustee for American Indians
- 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 configuration management, identity and access management, data protection and privacy, contingency planning, and incident response. KPMG made 18 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 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 2018 Performance Audit

February 22, 2019

KPMG LLP
1676 International Drive
McLean, Virginia 22102

KPMG LLP
1676 International Drive
McLean, VA 22102

February 22, 2019

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) 2018 *Federal Information Security Modernization Act of 2014 (FISMA)* Audit for unclassified information systems**.** We performed our work during the period of June 1 to September 30, 2018 and our results are as of November 20, 2018.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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.[1]

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

The audit objective(s) of our work for the year ending September 30, 2018 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) FY18 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 2018 FISMA Reporting Metrics for the OIG. Our sample was selected from information systems distributed across 11 Bureaus/Offices. These Bureaus/Offices are: the Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and

KPMG LLP is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), National Park Service (NPS), Office of Inspector General (OIG), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), the Office of the Special Trustee for American Indians (OST), 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.

In a FISMA performance audit, audit risk is the risk that auditors will not detect weaknesses in the design or implementation of an agency's information technology (IT) security controls. Such control weaknesses, if exploited, could have a serious adverse effect on agency operations, assets, or individuals and result in the loss of sensitive data. According to GAGAS, audit risk may be reduced by increasing the scope of work, changing the methodology to obtain additional evidence, obtaining higher quality evidence, or using alternative forms of corroborating evidence.

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. Specifically, we evaluated the implementation of 61 NIST-required security controls. We evaluated 61 (100%) of the controls by either interviewing Department/Bureau IT staff or reviewing Department/Bureau IT security control documentation. We evaluated four of 61 controls (6%) through testing by attempting to exfiltrate [1]sensitive data from DOI's network and by using software tools to measure security control effectiveness. DOI has a risk management and information system continuous monitoring programs. We identified needed improvements in areas audited including configuration management, identity and access management, data protection and privacy, contingency planning, and incident response.

The following table summarizes the control areas tested and the control deficiencies identified in the fiscal year 2018 FISMA Reporting Metrics for the OIG.

Cybersecurity Framework Security Functions[2]	Summary of Results
1. Identify (Risk Management)	DOI has established a risk management program.
2. Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training)	DOI has established configuration management, identity and access management, data protection and privacy, and security training programs. However, DOI has not fully: • [redacted] at BLM, BOR, and OST. • Performed [redacted] at BLM. • Reviewed third-party contractual agreement to ensure system changes were documented at BOR. • Implemented [redacted] within the prescribed timelines in accordance with DOI policy at BOR and USGS.

[1] Data exfiltration is the unauthorized transfer of data from a computer. Transfers can be automated and performed through programming over a network.

[2] 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.

	• [redacted] at OST. • [redacted] at BOR. • Documented processes to review or update position risk designations at BLM, FWS, and OSMRE. • Documented and implemented procedures to facilitate the implementation [redacted] at BIA, BOR, BSEE, FWS, NPS, OSMRE, and OST, [redacted]. • [redacted]
3. Detect (Information System Continuous Monitoring)	DOI has established an information system continuous monitoring program.
4. Respond (Incident Response)	DOI has established an incident response program. However, DOI has not fully: • Ensured personnel with incident response responsibilities complete training at BLM and BOR.
5. Recover (Contingency planning)	DOI has established a contingency planning program. However, DOI has not fully: • Documented and implemented procedures to ensure contingency planning lessons learned are maintained at BLM.

We have made 18 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 FY17 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 2018 questions for Inspector Generals.

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. This report is intended solely for the use of the DOI OIG and the DOI Office of the Chief Information Officer and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

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 11[3] Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2018:

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

4 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.

5 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.

6 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.

7 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.

8 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.

9 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.

[3]. Our sample resulted in a subset of information systems distributed over 11 Bureaus and Offices.

10 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.

11 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 Department has been without a CIO since September 2018.

The Deputy 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.

Bureaus and Offices have an Associate Chief Information Officer (ACIO) that reports to the CIO and the Deputy Bureau Director. The ACIO serves as the senior leader over all IT resources within the bureau or office. The Associate Chief Information Security Officer (ACISO) represent the bureau and office Information Assurance leadership and reports to the bureau ACIO and DOI CISO.

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 2018 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, 2018:

- 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 DOIOCIO as they relate to the FY2018 OIG FISMA reporting metrics; and
- An inspection of the information security practices, policies, and procedures in use across 11 Bureaus and Offices identified by the DOI OIG, specifically BIA, BLM, BOR, BSEE, FWS, NPS, OIG, OS, OSMRE, OST, 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.[4] The controls selected addressed areas covered by the DHS FY2018 Inspector General FISMA Reporting Metrics.

[4] In accordance with 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 11 of 128 operational systems of the total DOI information systems recorded in its official repository, the Cyber Security Assessment and Management tool (CSAM).

Table 1 describes the information systems audited.

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 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]	Moderate	[redacted]

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

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

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

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT			
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]

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

Results of Review

Our procedures identified improvements needed in the areas of configuration management, identity and access management, data protection and privacy, contingency planning, and incident response.
The details of the weaknesses we identified are as follows.

1. Implementation of the Configuration Management program.

The table below lists findings in the configuration management program.

FISMA domain	Summary of Findings
Configuration Management	DOI has not fully: • [redacted] at BLM, BOR, and OST. • Performed [redacted] at BLM. • Reviewed third-party contractual agreements to ensure system changes were documented at BOR. • Implemented [redacted] within the prescribed timelines in accordance with DOI policy at BOR and USGS. • Reviewed or updated [redacted].

KPMG performed the following procedures and noted the following weaknesses in four of 11 Bureaus and Offices' configuration management programs: BLM, BOR, USGS, and OST.

BLM:

KPMG obtained the population of security patches related to the [redacted]. From a population of 397 security patches, KPMG randomly selected 15 patches to examine to determine whether security patches were tested and approved prior to being implemented.

KPMG inquired of BLM management and was informed that updates and patches were tested and approved prior to implementation; however, BLM was unable to provide evidence the process was performed for the 15 selected samples.

During May of 2018, one change was made to [redacted] KPMG was informed by BLM that the system change was tested prior to deploying the change into the production environment; however, BLM was unable to provide evidence of the test.

Upon implementation of the change on May 1, 2018, end users of the system identified that a [redacted] and the Forms application of [redacted] could not be used. The service was restored on May 7, 2018 and required approximately one hour of downtime of [redacted]

KPMG was informed by BLM on 8/22/2018 that due to network bandwidth being prioritized for communications and support during peak fire season (April to September), there was insufficient bandwidth to run vulnerability scans on the [redacted]

BLM management opened POA&M ID [redacted] on 8/29/2018 specifically to address the [redacted]. Management has created milestones to add additional Microsoft

Vulnerability Manager (MVM) scan engines at the NOC and to create and install a dedicated [redacted].

BOR:

KPMG obtained and inspected a population of security-related patches applied to the BOR's respective systems. KPMG determined that documentation was not available to evidence the testing and approval of the patches during the period of October 1, 2017 through approximately July 15, 2018

KPMG obtained and inspected a population of application code changes applied to the [redacted] ystem. KPMG noted that from October 1, 2017 through approximately August 13, 2018 evidence of approval was maintained; however, documentation to support the occurrence of testing was not available.

USGS:

KPMG performed system security testing over the U.S. Geological Survey (USGS) [redacted] to determine whether [redacted] were remediated within established timeframes. The [redacted] provides virtual private cloud hosting services made available through a virtual data center that is used as needed by USGS application owners. [redacted] provides information resources that support the USGS science mission.

The USGS [redacted] consists of 42 servers and workstations and security vulnerabilities were identified on 29 of 42 (69%) devices. These devices are used to remotely access [redacted] in the [redacted] computing environment. Specifically, three critical, 20 high-risk, and 20 moderate-risk unique vulnerabilities were not remediated in accordance with the DOI Security Control Standards. The majority of the vulnerabilities impact the [redacted] The devices with the above weaknesses are not publicly accessible.

OST:

The OST [redacted] document, [redacted] document, and [redacted] document does not have a formal review process when updated. The following requirements are missing from the procedure documents:

- [redacted]: Document is missing required titles and their roles outlined in NIST SP800-128, Section 2.4. In addition, the document does not describe the process for [redacted] from unauthorized disclosure and modification.
- [redacted]: The document does not describe the process for implementing changes to secure configuration settings (baseline configurations).
- [redacted]: Document is missing a requirement that evidence of patch testing with appropriate approvals be maintained.

The Office of the Special Trustee for American Indians (OST) does document and retain results of testing and migration of patches onto the critical server environment. Patch testing is [redacted] in order to monitor for adverse effects. When deemed acceptable, [redacted]. There is no documentation to track the patch testing process and migration to the production environment.

DOI Security Control Standards Configuration Management, Version 4.1, CM-1 Configuration Management Policy and Procedures:

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; and

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.

DOI Security Control Standards Configuration Management, Version 4.1, CM-2 Baseline Configuration:

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Control Enhancements:

(1) *BASELINE CONFIGURATION | REVIEWS AND UPDATES*

The organization reviews and updates the baseline configuration of the information system:

(a) At least annually;

(b) When required due to a significant change; and

As an integral part of information system component installations and upgrades.

DOI Security Control Standard Configuration Management, Version 4.1, CM-3 Configuration Change Control

Control: The organization:

a. Determines the types of changes to the information system that are configuration-controlled;

b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;

e. Retains records of configuration-controlled changes to the information system for *System Owner-defined time period*;

f. Audits and reviews activities associated with configuration-controlled changes to the information system; and

g. Coordinates and provides oversight for configuration change control activities through *System Owner-defined configuration change control element (e.g., committee, board)* that convenes *(one or more) of System Owner-defined frequency*; *System Owner-defined configuration change conditions*.

Control Enhancement:

(2) *CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

DOI Security Control Standards Configuration Management, Version 4.1, CM-6 Configuration Settings:

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using United States Government Configuration Baseline, or other appropriate checklists from the National Vulnerability Database maintained by the National Institute of Standards and Technology, that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

DOI Security Control Standards Configuration Management, Version 4.1, CM-9 Configuration Management Plan:

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the information system and places the configuration items under configuration management; and

d. Protects the configuration management plan from unauthorized disclosure and modification.

DOI Security Control Risk Assessment, Version 4.1, RA-5 Vulnerability Scanning

Applicability: All Information Systems

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

Shares information obtained from the vulnerability scanning process and security control assessments with *System Owner-defined personnel or role*s to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

DOI Security Control Standards System and Services Acquisition, Version 4.1, SA-4 Acquisition Process

Applicability: All Information Systems

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;

b. Security strength requirements;

c. Security assurance requirements;

d. Security-related documentation requirements;

e. Requirements for protecting security-related documentation;

f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

DOI Security Control Standards System and Services Acquisition, Version 4.1, SA-10 Developer Configuration Management

Applicability: Moderate and High Impact Information Systems

Control: The organization requires the developer of the information system, system component, or information system service to:

a. Perform configuration management during system, component, or service [*Selection (one or more): design; development; implementation; operation*;

b. Document, manage, and control the integrity of changes to *System Owner-defined configuration items under configuration management*;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

Track security flaws and flaw resolution within the system, component, or service and report findings to *System Owner-defined personnel*.

DOI Security Control Standards System and Information Integrity, Version 4.1, SI-2 Flaw Remediation:

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 [Assignment: organization-defined time period] of the release of the updates; and

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

BLM: The [redacted] System Owner does not enforce the documentation of patches and updates applied to the [redacted] system. Per the System Owner, the [redacted] system relies on the Bureau to document patches applied to the system, which would include the testing and approval of the patch prior to it being implemented.

[redacted] management did not enforce the DOI configuration management policy to require testing and approvals prior to implementing a change into the production application.

There are network bandwidth limitations in the data pipe to [redacted] and during peak fire season the bandwidth is prioritized to support firefighters and fire support staff at the [redacted]. As such, the amount of network bandwidth to the [redacted] system is not sufficient to perform vulnerability scans.

BOR: Per inquiry with the Continuous Diagnostics and Mitigation Team Lead, the Bureau of Reclamation has made an effort to streamline its patching process. The bureau consolidates patches and implements these on a periodic basis. Additionally, the Information Technology Asset Configuration Team (ITACT), a working group, manages the process. The working group has attempted to streamline the patching process in order to remediate vulnerabilities in a more timely fashion, but the working group overlooked the need to document the testing of the patches applied to its various systems.

The [redacted] system owner does not require the vendor to document evidence that testing was performed prior to the vendor providing completed changes to the system owner. Per KPMG's inspection of the third-party contract in place with the mentioned vendor, KPMG noted that the contract does not explicitly require change testing to be documented.

USGS: A change in system administration personnel led to routine maintenance actions being overlooked. KPMG was informed that the [redacted] were considered [redacted] compared to other priorities that need to be addressed by limited system administrator resources.

OST: OST does not have a formal review process for documentation of configuration management, patch management, or change management procedures, or for maintaining written documentation over patch testing and testing results.

Lack of documenting the testing and approvals of security patches and updates before migrating to the production environment could lead to errors in the production environment.

Failure to perform testing and acquire approvals prior to implementing a change to the production environment could lead to the implementation of unauthorized changes in the system that could have adverse, unexpected results on the functionality of the application and/or and transactions expected by management.

BLM: A lack of [redacted] at the minimum required [redacted] increases the risk of the [redacted] system being compromised from the exploitation of a vulnerability.

A lack of [redacted] before migrating to the production environment could lead to potential error in the production environment.

USGS: Risks associated with the [redacted] system could lead to potentially inappropriate system access and a potential lost or disclosure of USGS information.

OST: Maintaining documented changes to configuration management, patch management, and change management procedures are necessary to eliminate confusion, create structure, and enforce uniform standards throughout a large group, and are most effective when clearly documented. A lack of approvals to these documented procedures can lead to potential errors in the production environment.

OST: Patches applied to the bureau's various systems are not documented, and this could lead to changes not adhering to the bureau's change management process. This could further lead to patches being applied to the production environment prior to being tested and approved. Additionally, this could lead to an increased security risk exposure due to a patch not being applied.

We recommend:

1. BLM enforce relevant policy and procedures related to updates and patch management to ensure testing and approvals are documented for BLM's [redacted] system prior to implementation.

2. BLM enforce configuration management policies and procedures for [redacted] to ensure that system changes are documented, approved, and tested prior to implementation to production.

3. BLM continue to work to expand network capacity in accordance with POA&M ID [redacted] to enable vulnerability scanning to be conducted for the [redacted] system.

4. BOR continue to enforce its change management policies and procedures to ensure that all update and patch testing applied to BOR's network and information systems is documented prior to the update or patch being implemented in the production environment.

5. BOR update its contractual agreement with its vendor to enforce the documentation of change testing for all changes that the vendor develops for the system. The updated contractual agreement should adhere to the bureau's change management policies and procedures to ensure that all change testing is documented prior to the change being implemented. The BOR, being the end user, should also test changes to validate the functionality of the change is what management is expecting.

6. USGS enhance [redacted] to ensure all [redacted] are applied in accordance with DOI policy. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.

7. OST:

a. Review and update the procedure documentation if applicable and require them to be reviewed and updated at least every two years going forward, to enforce DOI Security Control Standards for Configuration Management and requirements related to configuration management; and

b. Enforce these procedures and require evidence of testing and documentation to be maintained for all changes, patches, and baseline configurations.

8. OST enforce its change management policies and procedures to ensure that all patch testing and testing results are documented prior to the change being implemented. OST should maintain documentation (emails or tickets) showing the testing results for patches.

2. Implementation of the Identity and Access Management Program.

The table below lists findings in the identity and access management program.

FISMA domain	Summary of Findings
Identity and Access Management	DOI has not fully: • [redacted] at BOR. • Documented processes to review or update position risk designations at BLM, FWS, and OSMRE.

KPMG performed the following procedures and noted the following weaknesses in four of 11 Bureaus and Offices' identity and access management program: BOR, BLM, FWS, and OSMRE.

BOR:

BOR's [redacted]. During the audit, BOR had a script in place to automatically disable inactive accounts within Active Directory/Network with a last login date [redacted] and a password age greater than [redacted] Both criteria regarding password age and last login date must be met before the account is automatically disabled. On October 2, 2018, KPMG obtained and inspected evidence that the automatic account disabling script is now set to automatically disable accounts with a last login date [redacted] and a password age [redacted].

The BOR [redacted] system has eight users. KPMG sampled two of the eight users and determined they did not have the appropriate position risk designations assigned.

BLM:

KPMG was informed that BLM [redacted] BLM plans implement a process to review and update [redacted] by August 2019.

FWS:

FWS has not documented policies and procedures to establish their personnel security program. The DOI Personnel Security Control Standard requires FWS to develop, document and disseminate personnel security policy and procedures to all relevant parties.

More specifically, FWS lack documented procedures over the following processes:

- [redacted];
- [redacted];
- [redacted];
- [redacted]
- [redacted].

OSMRE:

KPMG reviewed the U.S. OSMRE Directives Systems, Information Systems Security Program procedures and determined that it lacked a process to periodically review the [redacted] to determine whether they are accurately identified.

Additionally, KPMG noted that the [redacted] spreadsheet that listed the user's [redacted] were not consistent with the suitability investigation requirements described in the directives. For example, the position title [redacted]

Additionally, KPMG randomly selected four users based on their position title and determined that three (3) of four (4) sampled FPPS records were inconsistent with the PDRs. See table 1 below for a summary of the results.

Table. Summary of result.

User	Position Title	OPM Position Designation Record	FPPS Record	Comment
User 1	[redacted]	[redacted]	[redacted]	[redacted].
User 2	[redacted]	[redacted]	[redacted]	[redacted].
User 3	[redacted]	[redacted]	[redacted]	[redacted]
User 4	[redacted]	[redacted]	[redacted]	[redacted]

DOI Security Control Standards Access Control, Version 4.1, AC-2 (3) Account Management | Disable Inactive Accounts, states:

"The information system automatically disables inactive accounts after 45 days."

DOI Security Control Standards Personnel Security, Version 4.1, PS-2 Position Risk Designation

Applicability: All Information Systems

Control: The organization:

a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations *at least every three years*.

DOI Security Control Standards Personnel Security, Version 4.1, PS-3 Personnel Screening

Applicability: All Information Systems

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and

Rescreens individuals according to *Office of Law Enforcement and Security (OLES) Personnel Security and Suitability Program investigation requirements*.

BOR Reclamation Manual Directives and Standards SLE 01-01

Position Designation. In accordance with OPM Federal Investigative Notice 10-06, the OPM PDT must be used to determine the position risk/sensitivity designation (i.e., the national security sensitivity and/or

suitability risk levels of a position.) This tool must be used in conjunction with the duties of the position identified in the PD and in collaboration with the supervisor/manager of the position.

Position Designation Levels**.** Each Reclamation position will be designated and the position designation level recorded on a position sensitivity designation sheet (generated from the OPM PDT), a PD cover sheet (OF-8), and in the Federal Personnel Payroll System (FPPS) at one of the risk or sensitivity levels identified in Table 1. In order to obtain Reclamation-wide consistency, several key Reclamation positions were designated through the use of the OPM PDT and the minimum position/risk sensitivity designation levels are identified in Appendix A (along with corresponding background investigation levels, security clearances, and pre-appointment background investigation waiver requirements).

BOR Reclamation Manual Directives and Standards SLE 01-01 Appendix A

Minimum Position Risk/Sensitivity Designations for Key Reclamation Positions or Assignments with Equivalent Duties Performed by Contractor Staff.

Table 2: Information Technology Positions. Based on the OPM PDT, the following position designations are identified below and retained in the servicing Human Resources Office. Background investigation and waiver requirements are also specified below.

Position or Position Category	**Minimum Designation Level**	**BI Level**	**BI Waiver Requirement**
IT or operations positions identified as having independent access to IT systems directly supporting water and power mission activities in the interest of public safety and well-being (e.g., SCADA system operators)	Moderate Risk Public Trust	Tier 2 (MBI)	Not Applicable
All other positions defined as having administrative-level (super-user) access to critical cyber assets	Moderate Risk Public Trust	Tier 2 (MBI)	Not Applicable

OSMRE Directives System
Subject: Information Systems Security Program
Chapter VII. Personnel Security/Suitability and Training: Computer/ADP Positions

OMB Circular A-130, Appendix III identifies these as positions involved in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. These include all positions classified in the GS-334 and GS-335 series as well as positions classified in other series where the majority of time is spent planning, designing, programming, operating or using computer systems, and similar contractor positions. This, however, would NOT include data entry or the collection of data using a computer, nor the development of specifications for what a program should do which are handed off to a computer specialist. Computer related designations would be as follows:

a. High Risk positions would be the senior management official for OSM computer operations that would be the Chief, ISM.

b. Moderate Risk positions would be a management or program official which has oversight or responsibility for a major portion of the overall OSM computer system. (LAN Administrators for the Regions, and Branch Chief or Program Managers within ISM.)

c. Low Risk positions would be those employees who have limited relation to the OSM mission or do not affect the efficiency of services and direction of the OSM.

Suitability Investigations:

Position Sensitivity Designation Level	Security Forms	Required Investigation	Required Reinvestigation
Low Risk	SF-85 & SF-87	NACI	None
Moderate Risk	SF-85P & SF-87	NACIC	None
High Risk	SF-85P & SF-87	BI	None

National Security Investigations:

Position Sensitivity Designation Level	Access Level	Security Forms	Required Investigation	Required Reinvestigation
Non-Critical Sensitive	Secret	SF-86 & FD-258 – Contractor SF-87 Federal	NACLC – Contractor ANACI – Federal	NACLC every 10 yr.
Critical Sensitive	Top Secret	DI-1912, SF-86, FD-258 – Contractor, SF-87 – Federal	SSBI	SBI-PR every 5 yr.

BOR: The [redacted] Since the creation, the Domain Administrators were unaware [redacted]. The [redacted]. The risk associated with this change was not formally accepted.

BLM: BLM did not develop and implement a comprehensive position risk determination process. The [redacted].

BOR: BOR Human Resources personnel determined the risk designation of the position based on the employees' job titles in [redacted] and the related Position Description. However, this [redacted]. Additionally, in the case of one of the two employees sampled for testing, the inspection of the [redacted].

FWS: FWS has not placed sufficient prioritization on the risks associated with a [redacted]

BOR: Disabling accounts upon reaching a last login date [redacted] helps ensure least privilege and that access is only maintained by users who require it. An account with a last login date [redacted] may be indicative of a user who no longer requires their account or may not need access at this time. By not disabling accounts with a last login date [redacted], unnecessary accounts remain active

and could be exploited or misused with the potential risk of compromise for a given account increasing each day beyond the [redacted] requirement.

BLM: Without a process to [redacted].

BOR: Without a proper understanding of the responsibilities an employee will fulfill, HR cannot accurately assign a position risk level, [redacted]. Such a lack of proper screening and background investigations could put critical assets at risk of a cyber-attack.

BOR: As a result of the [redacted] to the sampled users, background investigations for both users was a [redacted] although BOR requires a [redacted] in order to access the system. Additionally, because their position was incorrectly designated [redacted], re-screening procedures were not performed.

FWS and OSMRE: Without establishing a consistently implemented and effective [redacted] the risks associated with each [redacted]. As a result, users with [redacted] The [redacted] are accurate.

We recommend:

9. BOR approve and document any future changes to [redacted], in accordance with DOI Security Control Standards and other applicable policy requirements.

10. BLM implement a process to periodi[redacted].

11. BOR:

    a) Implement a process to periodically [redacted]

    b) Ensure compliance with the processes defined in the BOR Reclamation Manual Directives and Standards SLE 01-01 whereby BOR Human Resources assigns [redacted] in accordance with the Reclamation Manual Directives and Standards.

12. FWS document and implement [redacted] associated controls.

13. OSMRE to enhance their [redacted] are consistent with the position risk descriptions.

3. Implementation of the Data Protection and Privacy Program.

The table below lists findings in the data protection and privacy management program.

FISMA domain	Summary of Findings
Data Protection and Privacy	DOI has not fully: • Documented and implemented procedures to [redacted] • [redacted].

KPMG performed the following procedures and noted the following [redacted].

DOI has established a policy for protecting the confidentiality and integrity of [redacted]

KPMG inquired of Bureau and Office management and was informed that seven of 11 [redacted]

KPMG did not perform any further testing over the in-scope information systems to determine the control implementation status. Table 1 below lists the in-scope Bureaus, Offices, and their respective information systems.

Table 1. In-Scope Bureaus and Offices

Bureau/Office	Information System
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

KPMG performed a technical security test to determine whether security controls were effectively implemented in order to monitor and prevent sensitive data from being transmitted from the [redacted] to a remote KPMG computer. Using the [redacted] - to a remote KPMG computer. [redacted]

- File #1: [redacted].
- File #2: [redacted].
- File #3: [redacted].

Although testing was performed at [redacted] similar results could potentially be identified at other bureaus and offices from the FISMA sample of systems.

At the conclusion of the testing, KPMG inquired of [redacted] management to determine whether [redacted] detected the testing activity. DOI maintains the [redacted], which the bureaus and offices leverage to support their missions. In addition, the [redacted] is responsible for detecting and responding to security incidents department wide. KPMG was informed that [redacted].

Office of Management and Budget (OMB) Circular A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources* states:
"3.I.14. Encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is acceptable by the authorizing official and approved by the agency CIO, in consultation with the SAOP;
3.I.15. Implement the current encryption algorithms and validated cryptographic modules in accordance with NIST standards and guidelines;"

DOI Security Control Standards System and Communication Protection, SC-28 Protection of Information at Rest, states:

Applicability: Moderate and High Impact Information Systems

Control: The information system protects the Selection (one or more): confidentiality; integrity of System Owner-defined information at rest.

DOI Security Control Standard, System and Information Integrity, SI-4 Control Enhancement 4, states:

Information System Monitoring | Inbound and Outbound Communication Traffic

The information system monitors inbound and outbound communications traffic *System Owner-defined frequency* for unusual or unauthorized activities or conditions, including the unauthorized exporting of information.

Applicability: All Information Systems

Bureaus and Offices have [redacted].

The Department security controls that are [redacted].

[redacted]. In addition, DOI will be unable to determine their compliance with the relevant NIST controls and OMB requirements and puts DOI at risk of incidents related to the potential disclosure of sensitive information. Such an incident has the potential to have a negative impact on the Bureaus and Offices, the subject matter of the sensitive information disclosed, and the public's trust in DOI.

Risks associated [redacted].

We recommend:

14. [redacted]. The procedures should include roles and responsibilities, technical requirements, and exceptions to procedures when appropriate.

15. DOI [redacted].

4. Implementation of the Contingency Planning Program.

The table below lists findings in the contingency planning program.

FISMA domain	Summary of Findings
Contingency Planning	DOI has not fully: • [redacted].

KPMG performed the following procedures and noted the following weaknesses in one of 11 Bureaus and Offices' contingency planning program:

KPMG reviewed the [redacted] and noted it [redacted] requirement to document lessons learned within an After-Action Report following a live test exercise. Therefore, management [redacted].

NIST SP 800-34, Section 4 Reconstitution Phase, Appendix A, 5.7 Event Documentation

Control:

It is important that all recovery events be well documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP Coordinator.

Provide details about the types of information each ISCP team member is required to provide or collect for updating the ISCP with lessons learned. Types of documentation that should be generated and collected after a contingency activation include:

- Activity logs (including recovery steps performed and by whom, the time the steps were Initiated and completed, and any problems or concerns encountered while executing activities);
- Functionality and data testing results;
- Lessons learned documentation; and
- After Action Report.

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.

The contingency plan for the [redacted] within an After-Action Report following the live test exercise. Additionally, KPMG was informed that [redacted]

[redacted]

Additionally, the [redacted] order to continuously improve the plan for future contingency events. As a result, the system may become [redacted] to address future contingency events.

We recommend:

16. BLM update the [redacted].

5. Implementation of the Incident Response Program.

The table below lists findings in the incident response program.

FISMA domain	Summary of Findings
Incident Response	DOI has not fully: • [redacted]

KPMG performed the following procedures and noted the following weaknesses in two of 11 Bureaus and Offices' incident response program: [redacted].

[redacted]

KPMG reviewed the [redacted].

[redacted]

KPMG reviewed the [redacted].

DOI Security Control Standard Incident Response, Version 4.1, IR-2 Incident Response Training

Applicability: All Information Systems

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. *Prior to* assuming an incident response role or responsibility;

b. When required by information system changes; and

c. *At least annually* thereafter.

[redacted].

[redacted].

Technology has an ever changing landscape. Effective training will bring greater awareness and new knowledge to address changes. The annual incident response exercises are beneficial; however, without ensuring that all necessary individuals are completing incident response training, the members of the incident response team may not be prepared to address situations. As a result, systems may become more vulnerable to attack or failure.

Without incident response training, [redacted]. Additionally, controls are

more likely to be performed incorrectly. As a result, incidents can potentially lead to additional data loss, data exposure, data corruption, etc.

We recommend:

17. [redacted].

18. [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 configuration management, identity and access management, data protection and privacy, contingency planning and incident response.

Management Response to Report

The following is the Department responses to the report recommendations.

Recommendation #1 Response: The BLM concurs with this recommendation. The BLM will implement [redacted] BLM will communicate requirement(s) with the system owners; track progress of configuration management procedure implementation; review artifacts for sufficiency; document implementation in the Weakness Completion Verification Form (WCVF). Target Completion Date: 12/31/2019.

Recommendation #2 Response: The BLM concurs with this recommendation. The BLM will implement [redacted]. BLM will communicate requirement(s) with the system owners; track progress of configuration management procedure implementation; review artifacts for sufficiency; document implementation in the Weakness Completion Verification Form (WCVF). Target Completion Date: 12/31/2019.

Recommendation #3 Response: The BLM concurs with this recommendation. The BLM will implement [redacted]. BLM will communicate requirement(s) with the system owners; track progress of configuration management procedure implementation; review artifacts for sufficiency; document implementation in the Weakness Completion Verification Form (WCVF). Target Completion Date: 5/31/2019.

Recommendation #4 Response: The BOR concurs with this recommendation. The BOR has already implemented and will continue to enforce its [redacted]. On September 19, 2018, BOR provided KPMG documentation evidencing that the [redacted]. Completion date 9/9/2018 (Implemented).

Recommendation #5 Response: The BOR concurs with this recommendation. A Plan of Action and Milestones (POA&M) will be created for [redacted]. The BOR will develop procedures to ensure that [redacted] Target Completion Date: 1/15/2020.

Recommendation #6 Response: The USGS concurs with this recommendation. The USGS developed a [redacted]. January 2019 is the effective date for this plan and the following corrective actions:

- New [redacted] as required by DOI policy.
- [redacted].
- [redacted]. If required

remediation timelines cannot be met, then [redacted]. Target Completion Date: 6/30/2019.

Recommendation #7 Response: The OST concurs with this recommendation. The OST will implement [redacted]. Target Completion Date: 6/30/2019.

Recommendation #8 Response: The OST concurs with this recommendation. The OST will implement internal controls to [redacted]. Target Completion Date: 6/30/2019.

Recommendation #9 Response: The BOR concurs with this recommendation. The BOR already implemented and continues to ensure [redacted] The BOR took action and updated [redacted]. The evidence was provided to KPMG on October 2, 2018. Completion Date: 10/2/2018 (Implemented).

Recommendation #10 Response: The BLM concurs with this recommendation. The BLM will implement a process to [redacted] BLM will communicate requirement(s) with the system owners; track progress of configuration management procedure implementation; review artifacts for sufficiency; document implementation in the Weakness Completion Verification Form (WCVF). Target Completion Date: 2/28/2020.

Recommendation #11 Response: The BOR concurs with this recommendation. The BOR will implement a process to [redacted]. Additionally, BOR will ensure compliance with the [redacted]. Target Completion Date: 12/31/2019.

Recommendation #12 Response: The FWS concurs with this recommendation. The FWS's Information [redacted] Target Completion Date: 6/30/2019.

Recommendation #13 Response: The OSMRE concurs with this recommendation. The OSMRE has initiated a comprehensive revision of the current bureau directive, [redacted]. Target Completion Date: 6/30/2019.

Recommendation #14 Response: The DOI's Office of the Chief Information Officer (OCIO) will ensure bureaus/offices develop plans to address this deficiency and will track bureau/office progress to ensure compliance with policy, where feasible. If policy compliance is not possible and/or would negatively affect the operations of a system, DOI will develop a waiver process to ensure risks are documented and approved. Target Completion Date: 12/31/2019.

- The BIA concurs with this recommendation. The BIA will document procedures to [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

- The BOR concurs with this recommendation. The BOR will document procedures to [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

- The BSEE concurs with the recommendation. The BSEE will document procedures to [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

- The FWS concurs with this recommendation. The FWS will document procedures to [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

- The NPS concurs with this recommendation. The NPS will document procedures [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

- The OSMRE concurs with this recommendation. The OSMRE will document procedures to [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

- The OST concurs with this recommendation. The OST will document procedures to [redacted] Per the Department's response, these procedures will be reviewed by the OCIO for sufficiency and consistency. Target Completion Date: 12/31/2019.

Recommendation #15 Response: The Department concurs with this recommendation. [redacted] The completion of that project will implement this recommendation. Target Completion Date: 12/31/2019.

Recommendation #16 Response: The BLM concurs with this recommendation. The BLM will incorporate [redacted]. The BLM will communicate requirement(s) with the system owners; track progress of configuration management procedure implementation; review artifacts for sufficiency; and document implementation in the Weakness Completion Verification Form (WCVF). Target Completion Date: 12/31/19.

Recommendation #17 Response: The BLM concurs with this recommendation: The BLM will enforce adherence to its [redacted] BLM will communicate requirement(s) with the system owners; track progress of configuration management procedure implementation; review artifacts for sufficiency; and document implementation in the Weakness Completion Verification Form (WCVF). Target Completion Date: 12/31/2019.

Recommendation #18 Response: The BOR concurs with this recommendation. The BOR will develop a corrective action plan and create a POA&M to [redacted] Target Completion Date: 1/15/2020.

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 FY2018 CyberScope Responses.

The Identify function area consists of risk management. The Protect function area consists of configuration management, identity and access management, data protection and privacy 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	FWS	NPS	OIG	OS	OSMRRE	OST	USGS
Identify											
Protect	**X**	**X**	**X**		**X**			**X**	**X**	**X**	**X**
Detect											
Respond		**X**	**X**								
Recover		**X**									

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
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
CSAM	Cyber Security Assessment and Management
CVE	Common Vulnerability and Exposures
DHS	Department of Homeland Security
DOI	United States Department of the Interior
DRP	Disaster Recovery Plan
FCD	Federal Continuity Directive

Acronym	Definition
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
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
NIST	National Institute of Standards and Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

Acronym	Definition
OMB	Office of Management and Budget
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
SP	Special Publication
SSP	System Security Plan
ST	Security and Awareness Training
STIG	Security Technical Implementation Guide
TLS	Transport Layer Security
US	United States

Acronym	Definition
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 FY17 FISMA report recommendations and the status as of September 30, 2018.

Table 1. FY2017 FISMA Report Recommendations and Status as of September 30, 2018.
10 of 16 Recommendations are Open

Description	Status
1. BSEE: We recommend BSEE continue to fully implement risk management processes consistent with the approved ISCM strategy.	Closed. August 2, 2018
2. BSEE: Develop an enterprise architecture and subsequent information security architecture across the bureau, business process and system levels.	Closed. August 2, 2018
3. BSEE: 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.	Closed. August 2, 2018
3. NPS: Ether 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.	Open
3. 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.	Open
4. FWS: Enhance vulnerability management oversight to ensure all relevant and appropriate [redacted]. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.	Open
5: FWS: Enhance the vulnerability management process to [redacted].	Open
6. SOL: Enforce oversight compliance to ensure that all responsible parties are effectively reviewing, updating, and maintaining open POA&Ms in CSAM.	Closed. June 14, 2018
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.	Closed. June 14, 2018
8. BSEE: Continue to fully implement the ISCM strategy across both organizations and respective information systems.	Closed. August 2, 2018
9. BSEE: 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's ISCM program and identify areas for improvement, as required.	Closed. August 2, 2018

10. OST: Develop a process to ensure [redacted].	Closed. August 28, 2018
11 – 16. BLM: 11. [redacted] 12. [redacted]. 13. Implement a process to perform [redacted] Ensure that changes [redacted]. 14. Implement other methods to [redacted], such as: [redacted]; [redacted]. 15. [redacted]. 16. Implement a process to [redacted].	Open
17. OST: Update the [redacted].	Closed. August 23, 2018
18. BOR: Develop procedure documentation [redacted] At a minimum, the procedure document should include the following elements: [redacted]	Closed. August 16, 2018
19 and 20. BLM	Closed. May 30, 2018

19. Update [redacted] 20. BLM ensure that [redacted].	

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: Data Protection and Privacy	
NIST SP 800-53: SC-7	Boundary Protection

NIST SP 800-53: SC-8	Transmission Confidentiality and Integrity
NIST SP 800-53: SC-28	Protection of Information at Rest
NIST SP 800-53: MP-3	Media Marking
NIST SP 800-53: MP-6	Media Sanitization
NIST SP 800-53: SI-3	Malicious Code Protection
NIST SP 800-53: SI-4	Information System Monitoring
NIST SP 800-53: SI-7	Software, Firmware, and Information Integrity
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 2018 Questions for Inspectors General

The information included represents the Department of the Interior (DOI) responses to Department of Homeland Security's (DHS) FISMA 2018 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 2018 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 2018 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.

Function 0 is the overall summary for the FISMA Performance Audit for DOI. Functions 1–5 follow the five Cybersecurity Functions, Identify, Protect, Detect, Respond and Recover.

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, 2018. The scope of the audit included the following Bureaus

and Offices, Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), National Park Service (NPS), Office of the Inspector General (OIG),

Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), Office of the Special Trustee for American Indians (OST), and U.S. Geological Survey (USGS). DOI had 123 operational unclassified information systems and 11 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, data protection and privacy, information security continuous monitoring, incident response, and contingency planning metric domains. Consistent with the Fiscal Year (FY) 2018 OIG FISMA metric rating instructions, ratings throughout the eight 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 Protect function at Managed and Measurable (Level 4). The Identify, Detect, and Recover at Consistently Implemented (Level 3). The Respond function was assessed at Defined (Level 2). Overall, DOI was assessed at Consistently Implemented (Level 3).

Function 1: Identify – Risk Management

1 To what extent 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, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Maturity Level: Managed and Measureable (Level 4). The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.

DOI maintains an inventory of its information systems in the [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. Information systems are also subject to continuous monitoring as described in the continuous monitoring plan.

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; FY 2018 CIO FISMA Metrics: 1.2)?

Maturity Level: Managed and Measurable (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.

DOI uses several automated tools to monitor hardware assets connect to the network. Information systems are also subject to continuous monitoring as described in the continuous monitoring plan.

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: Managed and Measurable (Level 4) – The organization ensures that the software assets on the network (and their associated licenses) are subject to the monitoring processes defined within the organization's ISCM strategy.

DOI utilizes manual and automated processes to maintain an inventory of software assets and ensures the inventory is periodically monitored. Additionally, DOI is in the process of implementing a [redacted] software solution as part of their software asset management suite of tools.

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; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

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.

Ten of 11 Bureaus and Office, [redacted] have consistently defined their mission and business functions in their respective risk management policies and procedures. [redacted], which is scheduled to be completed December 31, 2018. 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 includes 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 SP 800-39; NIST SP 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; FY 2018 CIO FISMA Metrics: 1.6)?

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.

Seven of 11 Bureaus and offices, [redacted] have [redacted], [redacted].

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

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk , including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

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.

Ten of 11 Bureaus and Offices, [redacted] have implemented a [redacted] is in the process of implementing its [redacted]. DOI can improve its maturity level by ensuring that eight Bureaus and Offices, [redacted] incorporate [redacted].

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, 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 SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Maturity Level: Managed and Measurable (Level 4) - 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.

DOI has defined roles and responsibilities of risk management stakeholders such as the Chief Information Officer, Chief Information Security Officer, System Owner, and Authorizing Official. Additionally, DOI established the Information Management Technology Leadership Team that consists of the Bureau and Office Directors of Information Security, DOI Information Assurance Leadership Team, and the Compliance and Audit Management Branch.

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.

The Bureaus and Offices have implemented POA&Ms in accordance with the DOI POA&M Process Standards. However, [redacted] have not defined [redacted]. The Department can improve its security maturity level by defining [redacted]

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) security controls to mitigate system-level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 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.

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; OMB Circular A-11; Green Book (Principles #9, #14 and #15))?

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.

DOI has consistently communicated risks in a timely manner to stakeholders such as Directors of information Security, Chief Information Security Officers, System Owners, and System Administrators. Communication methods include email and various security working group 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, roles and responsibilities for reporting, including dashboards that facilitate a portfolio view of risk across the organization.

DOI can improve and increase its maturity level by developing and implementing a diagnostic and reporting framework, including dashboards to facilitate a portfolio view of risks 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, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

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.

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, this recommendation remains open. DOI indicated that the recommendation is scheduled to be fully implemented December 31, 2018. 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.

Seven of 11 Bureaus and Office, [redacted] have implemented a bureau-level solution that provides a centralized view of risk and management dashboards. [redacted], [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, [redacted] 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 affect to DOI systems and data.

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

The maturity level for the Risk Management function was assessed at Consistently Implemented (Level 3). Seven of 12 risk management metrics were assessed at Level 3: Consistently Implemented. Four of 12 risk management metrics were assessed at Level 4: Managed and Measurable. One of four risk management metrics were assessed at Leve 1: Ad hoc.

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?

No additional testing was performed beyond the above metrics. Based on the consistently implemented maturity level, the DOI 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; NIST 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. This is the highest maturity level available for this metric.

DOI has resources to adequately implement the information system configuration management activities.

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 phase within an organization's SDLC ; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 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.

DOI disseminated configuration management related policies and required the Bureaus and Offices to implement procedures to support the configuration management program. Bureaus and Offices have implemented organizational or system specific configuration management plans. However, nine of 11 Bureaus and Offices, [redacted] have not defined, monitored, or reported qualitative and quantitative performance measures on the effectiveness of the configuration management program. [redacted] have not [redacted]. In addition, 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 SP 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.

Ten of 11 Bureaus and Offices, [redacted] have implemented policies and procedures for managing the configuration of its information system. However, [redacted] did not review or update their [redacted] Additionally, 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 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; 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.

Ten of 11 Bureau and Offices, [redacted] have implemented configuration management change control in accordance with Department Security Control Standards. However, [redacted] did not [redacted], in accordance with DOI Security Control Standards. In addition, DOI is in the process of implementing an automated solution for application whitelisting.

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 2018 CIO FISMA Metrics: 1.1 and 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]

Ten of 11 Bureaus and Offices, [redacted] have developed, documented, and disseminated its policies and procedures and maintained configuration build guides. However, [redacted] did not review or update [redacted]. Automated tools are used to scan information systems for code-based and configuration-based vulnerabilities. DOI can improve its maturity level by implementing technology that maintains security configurations 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 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; 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.

DOI is managing its flaw remediation process and utilizes patch management and software update tools for operating systems and third-party applications. The technology is [redacted] Four of 11 Bureaus and Offices, [redacted].

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (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.

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 SP 800-53: CM-2 and 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.

Nine of 11 Bureaus and Offices, [redacted] have implemented change control policies and procedures. [redacted]. Two of 11 Bureaus and Offices, BOR and BLM [redacted]

In addition, 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 maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

No additional testing was performed beyond the above metrics. Seven of eight configuration management metrics were assessed at Consistently Implemented. One of eight configuration management metrics were assessed at Level 4: Managed and Measurable. 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 SP 800-53: AC-1, IA-1, and PS-1; 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.

DOI has defined its identity, credential, and access management roles and responsibilities through Departmental policies and manuals. In addition, a DOI Access Executive Steering Committee was established to oversee the program. This is the highest maturity level for the metric.

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

Maturity Level: Managed and Measurable (Level 4) – The organization has transitioned to its desired or "to-be" ICAM architecture and integrates its ICAM strategy and activities with its enterprise architecture and the FICAM segment architecture.

DOI has implemented and manages the Department of the Interior Personal Identity Verification (PIV) credentials, DOI Access Cards and integrated the technology into its Active Directory network infrastructure.

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 26 through 31) (NIST SP 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Maturity Level: Consistently Implemented (Level 3) – The organization consistently implements its policies and procedures for ICAM, including for account management, separation of duties, least privilege, remote access management, identifier and authenticator management, and identification and authentication of non-organizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies and procedures, and processes to update the program.

Ten of 11 Bureaus and Offices, [redacted] have implemented a process to manage the implementation of its policies and procedures. However, [redacted]

not consistently disable inactive user accounts in accordance with DOI Security Control Standards. DOI can improve and increase its maturity level by capturing lessons learned and implementing automated mechanisms to manage the effectiveness of its ICAM policies and procedures.

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 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Maturity Level: Defined (Level 2) – The organization has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. Processes have been defined for assigning risk designations for all positions, establishing screening criteria for individuals filling those positions, authorizing access following screening completion, and rescreening individuals on a periodic basis.

Four of 11 Bureaus and Offices, [redacted] did not consistently define procedures for assigning personnel risk designations or update procedures to ensure they are consistent with current operations. [redacted].

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.

Through automation, DOI reviews and maintains access agreements such as rule of behavior for individuals prior to granting system access. DOI can improve and increase its maturity level by using automation to manage and review nondisclosure agreements for users.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

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

DOI utilizes strong authentication for authenticating 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 (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 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; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

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

DOI has 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. 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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and 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.

Ten of 11 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. [redacted] This is the highest maturity level available.

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 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

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.

DOI has effectively implemented technology over end user mobile workstations that performs a series of host-based security checks prior to allowing remote access and restricts data transfer to authorized DOI computing environments with Virtual Private Network software.

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?

No additional testing was performed beyond the above metrics. Managed and Measurable (Level 4): Five of nine IAM related metrics were assessed at Managed and Measurable (Level 4). Three of nine IAM metrics were assessed at Consistently Implemented (Level 3). One of nine IAM metrics was assessed at Defined (Level 2). The IAM program is effective.

Function 2C: Protect – Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Maturity Level 3: Consistently Implemented. The organization consistently implements its privacy program by: Dedicating appropriate resources to the program maintaining an inventory of the collection and use of PII Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems. Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs)

Nine of 11 Bureaus and Offices, [redacted] have developed and implemented a privacy program for the protection of personally identifiable information (PII). [redacted] DOI can improve its maturity level by developing and monitoring quantitative and qualitative performance measures on the effectiveness of its privacy activities and conducting an independent review of its privacy program.

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

- Encryption of data at rest
- Encryption of data in transit
- Limitation of transfer to removable media
- Sanitization of digital media prior to disposal or reuse

Maturity Level 1: Ad Hoc. The organization has not defined its policies and procedures in one or more of the specified areas.

Eight of 11 Bureaus and Offices, [redacted].

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Maturity Level 2: Defined. The organization has defined and communicated it policies and procedures for data exfiltration and enhanced network defenses.

DOI has implemented Security Incident and Event Managing software, firewalls, network monitoring tools, email filtering, and packet inspection software to monitor for unusual network activity. However, DOI does not conduct exfiltration exercises to measure the effectiveness of its data exfiltration network defenses. Additionally, KPMG performed a data exfiltration exercise over two of 11 Bureaus and Offices, BIA and USGS and determined that USGS or the DOI security operation center did not prevent the activity.

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Maturity Level 4: Managed and Measurable. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

DOI has established a Data Breach Response Plan and periodically performs exercises and makes improvements to the plan as needed. In addition, DOI monitors performance measures on the effectiveness of its Data Breach Response Plan as appropriate.

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)?

Maturity Level 3: Consistently Implemented. The organization ensures that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually. Additionally, the organization ensures that individuals certify acceptance of responsibilities for privacy requirements at least annually.

DOI tracks and monitors basic privacy awareness training and maintains a role-based privacy training self-certification module in the DOI Learning Management System. DOI periodically performs phishing exercises but those responsible for PII are not specifically targeted.

38 Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy 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 data protection and privacy program effective?

No additional testing was performed beyond the above metrics. The data protection and privacy program is not effective. Two of five data protection and privacy metrics were assessed at consistently implemented (Level 3). One of five data protection and privacy metrics were assessed at managed and measurable (Level 4). One of five data protection and privacy metrics were assessed at defined (Level 2). One of five data protection and privacy metrics were assessed at ad hoc (Level 1)

Function 2D: Protect – Security Training

39 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 SP 800-53: AT-1; and NIST SP 800-50).
Maturity Level: Consistently Implemented (Level 3) - Roles and responsibilities for stakeholders involved in the organization's security awareness and training program have been defined and communicated across the organization. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities.

DOI has established a security training program that is supported with associated policies and procedures. Roles and responsibilities are defined and requirements disseminated to the Bureaus and Offices annually. This is the highest level for this metric.

40 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 SP 800-53: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?
Maturity Level: Managed and Measureable (Level 4) – The organization has addressed its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors.

DOI conducted a workforce assessment to identify the knowledge, skills, and specialized security training needed to support its security program. DOI has either addressed or is actively addressing knowledge, skill, or abilities gaps.

41 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 SP 800-53: AT-1; NIST SP 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.

DOI monitors compliance and periodically performs phishing exercises to measure effectiveness of the security awareness and training program. Performance is measured in the DOI Learning 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 that need to be made to the security awareness and training program.

42 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 of questions 43 and 44 below) (NIST SP 800-53: AT-1 through AT-4; and NIST SP 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.

DOI monitors and analyzes specialized and role-based security training performance measures over its security awareness and training program. Performance is captured in the DOI Learning 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 and procedures, and program to a changing cybersecurity landscape and provides awareness and training, as appropriate, on evolving and sophisticated threats.

43 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 SP 800-53: AT-2; FY

2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Maturity Level: Managed and Measurable (Level 4) - The organization measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.

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 Learning management system. In addition, DOI measures the effectiveness of its security awareness training program by periodically performing phishing exercises.

44 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 SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Maturity Level: Managed and Measurable (Level 4) - The organization obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.

DOI ensures that staff with significant security responsibilities such as the Associate Chief Information Officer, Authorizing Official, and System Owner perform role-based security training at least annually. Training records are maintained in the centralized DOI Learning management system. In addition, DOI measures the effectiveness of its security awareness training program by periodically performing phishing exercises.

45.1 Please provide the assessed maturity level for the agency's Protect Function.

The maturity level for the Protect function was assessed at Managed and Measurable (Level 4) Two of Four functional areas, Configuration Management, and Data Protection and Privacy were assessed at Consistently Implemented (Level 3). Identity and Access Management and Security Training were assessed at Managed and Measurable (Level 4). Configuration Management, seven of eight metrics were assessed at Consistently Implemented (Level 3). Identity and Access Management, five of nine metrics were assessed at Managed and Measurable (Level 4). Data Protection and Privacy, three of five metrics were assessed at Consistently Implemented (Level 3). Security Training, four of six metrics were assessed at Managed and Measurable (Level 4).

45.2 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?

No additional testing was performed beyond the above metrics. Five of six security training metrics were assessed at Managed and Measurable (Level 4) and one of six security training metrics was assessed at consistently implemented (Level 3). DOI assessed the skills and specialized training required to support its cybersecurity related activities. DOI monitors general and role-based security and awareness training performance and periodically performs phishing exercises. The security training program is effective.

46 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.

DOI has established an information security continuous monitoring (ISCM) strategy. Seven of 11 Bureaus and Offices, [redacted]. Four of 11 Bureaus and Offices, [redacted]

47 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; collection of 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 49)?

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.

DOI has implemented an ISCM program. However, seven of 11 Bureaus and Offices [redacted]

48 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 2018 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.

DOI has implemented an ISCM program and defined roles and responsibilities and dependencies are defined. Seven of 11 Bureaus and Offices [redacted]

49 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 security control assessments and plan of action and milestones.

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

Maturity Level: Consistently Implemented (Level 3) - The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.

Seven of 11 Bureaus and Offices, [redacted]

51.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

The maturity level for the ISCM function was assessed at Consistently Implemented (Level 3). Four of five ISCM metrics were assessed at Consistently Implemented (Level 3). One of five ISCM metrics were assessed at Managed and Measurable (Level 4).

51.2 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?

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

52 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 SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58)?

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.

DOI has implemented an incident response program. The DOI Enterprise Computer Security Incident Response Plan program defines the policies and procedures. However, KPMG performed a data exfiltration exercise over two of 11 Bureaus and Offices, [redacted]. Also, the Bureaus and Offices have [redacted].

53 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: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Maturity Level: Consistently Implemented (Level 3) – Defined roles and responsibilities are consistently implemented and teams have adequate resources (people, processes, and technology) to consistently implement incident response activities.

DOI has implemented an incident response program. The DOI Enterprise Computer Security Incident Response Plan program defines the policies and procedures. However, the Bureaus and Offices [redacted].

54 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; OMB M-18-02; and 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.

DOI has implemented its incident response processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated, reviewed, and prioritized. However, DOI [redacted]. Specifically, KPMG performed a data exfiltration exercise over two of 11 Bureaus and Offices, [redacted]

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?

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.

KPMG performed a technical security test at two Bureaus and Offices, [redacted].

56 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-18-02; NIST SP 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

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.

The [redacted] 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.

57 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, including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Maturity Level: Managed and Measurable (Level 4) - The organization utilizes [redacted] to detect and proactively block cyber-attacks or prevent potential compromises.

When appropriate, DOI has the capability to leverage the services of DHS and other organizations for additional incident response capability. DOI has fully implemented [redacted] capabilities.

58 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; NIST SP 800-44)

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.

DOI has implemented tools and technology to support the incident response program such as firewalls, malware detection, data loss prevention technology, and endpoint server security tools. DOI is in the process of implementing an enterprise-level security information and event management product and solution.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.
Defined (Level 2). Three of seven incident response metrics were assessed at Defined (Level 2). Two of seven incident response metrics were assessed at Consistently Implemented (Level 3). Two of seven incident response metrics were assessed Managed and Measurable (Level 4).

59.2 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?

No additional testing was performed. The incident response program is not effective.

Function 5: Recover – Contingency Planning

60 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 SP 800-53: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Maturity Level: Consistently Implemented (Level 3) - 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. This is the highest maturity level available.

DOI has established a contingency plan program that requires each information system to maintain an information system contingency plan. Information system contingency plans address contingency roles, responsibilities, and identifies business functions and associated requirements. Teams are assigned specific roles in contributing to the recovery of the information system and trained to respond to a contingency event.

61 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 62-66) (NIST SP 800-34; NIST SP 800-161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

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.

Four of 11 Bureaus and Offices, [redacted] have implemented information system contingency planning policies and procedures in accordance with DOI Security Control Standards and considered supply chain risks. Lessons learned are communicated in the results of annual contingency plan tests and exercises.

Four of 11 Bureaus and Offices, [redacted].

[redacted]. The [redacted] conducted a contingency plan exercise in fiscal year 2018; however, [redacted]

DOI can improve and increase its maturity level by ensuring Bureaus and Offices understand and manage its information and communication technology (ITC) supply chain risks related to contingency planning activities. As appropriate, Bureau and Offices should 1) consider supply chain concerns into its contingency planning policies and procedures, 2) define and implement a contingency plan for its ICT supply chain infrastructure, 3) apply appropriate ICT supply chain controls to alternate storage and processing sites, and 4) consider alternate telecommunication service providers for its ICT supply chain infrastructure and to support critical information systems.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

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.

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

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

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.

DOI consistently implemented information system contingency plans in accordance with DOI Security Control Standards. DOI [redacted].

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

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.

10 of 11 Bureaus and Offices, [redacted] have implemented contingency plan testing and exercises. [redacted].

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2018 CIO FISMA Metrics: 5.4; 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.

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

66 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 SP 800-53: CP-2 and IR-4)?

Maturity Level: Managed and Measurable (Level 4) - Metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and the organization has ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

DOI participated in the annual Eagle Horizon exercise, which is an exercise to evaluate the department's recovery ability for mission essential functions and related information systems. Test results and lessons learned are shared with senior DOI leadership, Bureaus, and Offices.

[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.

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

The Contingency Planning function was assessed at Consistently Implemented (Level 3). Six of seven metrics were assessed at Consistently Implemented (Level 3). One of seven metrics were assessed at Managed and Measurable (Level 4).

67.2 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?

No additional testing was performed beyond the above metrics. The contingency planning 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