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 2019

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

Report No.: 2019-ITA-034 February 2020

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

FEB 2 6 2020

Memorandum

To: William E. Vajda
Chief Information Officer

From: Mark L. Greenblatt
Inspector General

Subject: *Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2019*
Report No. 2019-ITA-034

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) 2019. 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, at the OIG's discretion, to determine the effectiveness of such programs and practices.

KPMG, an independent public accounting firm, performed the DOI FY 2019 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. The OIG does not express an opinion on the report, nor on KPMG's conclusions regarding the 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 risk management, configuration management, identity and access management, and contingency planning. KPMG made 27 recommendations related to these control weaknesses intended to strengthen the Department's information security program, as well as those of the Bureaus and Offices. In its response to the draft report, the Office of the Chief Information Officer concurred with all recommendations and established a target completion date for each corrective action.

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

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

Attachment

The United States Department of the Interior
Office of Inspector General
Federal Information Security Modernization Act of 2014
Fiscal Year 2019 Performance Audit

January 29, 2020

KPMG LLP
8350 Broad Street
McLean, Virginia 22102

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

January 29, 2020

Mr. Mark Lee Greenblatt
Inspector General
U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW MS 4428
Washington, DC 20240-0001

Dear Mr. Greenblatt:

This report presents the results of our work conducted to address the performance audit objectives relative to the Fiscal Year (FY) 2019 *Federal Information Security Modernization Act of 2014 (FISMA)* Audit for unclassified information systems**.** We performed our work during the period of May 20 to September 30, 2019 and our results are as of November 4, 2019.

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.

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, 2019 were to:

- Perform the annual independent FISMA audit of the Department of the Interior (DOI) 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 2, 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) FY19 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 the overall security program.

Our procedures tested security control areas identified in NIST SP 800-53 and additional security program areas identified in the 2019 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 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. DOI has a risk management and information system continuous monitoring program. We identified needed improvements in areas audited including Risk Management (RM), Configuration Management (CM), Identity and Access Management (IAM), and Contingency Planning (CP).

Metrics are 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.

The following table summarizes the control areas tested and the control deficiencies identified in the fiscal year 2019 FISMA Reporting Metrics for the OIG.

Cybersecurity Framework Security Functions	Summary of Results
1. Identify (Risk Management)	DOI has established a risk management program. However, DOI has not fully: • Applied security controls appropriately and effectively document the justification for not implementing selected security controls at [redacted] • Documented and approved formal configuration management policies at [redacted] Completed remediation activities to ensure the Interagency Agreement template contains adequate language to meet the security requirements and contracting language required at [redacted] • Designed and implemented effective technical controls to detect indicators of potential attacks and prevent potential security incidents involving internal threats on the [redacted]

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 consistently: • Adhered to established configuration management procedures at [redacted] • Implemented an effective patch and vulnerability management process to remediate vulnerabilities identified in vulnerability assessment scans at [redacted] • Performed monthly vulnerability scanning and has not documented monthly vulnerability management procedures at [redacted] • Implemented a solution or documented procedures to monitor configuration settings and baseline configurations and documented procedures to support configuration baseline monitoring at [redacted] • Documented, tested, and approved security patches prior to being implemented at [redacted] • Reported [redacted] security patching information to the department in accordance with the department Continuous Diagnostics and Monitoring (CDM) initiative. • Completed the remediation of vulnerabilities identified on [redacted] • Implemented a formal user access authorization process for non-privileged users at the [redacted] • Reviewed system audit logs for unusual activity at [redacted] • Implemented an effective user account management review process at [redacted] • Implemented effective personnel screening procedures at [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.
5. Recover (Contingency planning)	DOI has established a contingency planning program. However, DOI has not fully: • Reviewed and updated information system contingency plans at [redacted] • Ensured business impact analysis templates meet federal requirements at [redacted]. • Conducted functional contingency plan tests or exercises, nor documented results for moderate impact information systems at [redacted].

We have made 27 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 FY18 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 2019 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.

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[1] Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2019:

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.

[1] 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 Department's Office of the Chief Information Officer (OCIO) leads the security management program for the Department. The Chief Information Officer (CIO) leads the OCIO and reports to the Department 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 assigned a new CIO in March 2019.

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. A new CISO was assigned in September 2019.

Bureaus and Offices have an Associate Chief Information Officer (ACIO) that reports to the Department 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 DOI. 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 2019 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, 2019:

- Perform the annual independent 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/DHS FISMA Reporting Metrics on behalf of the DOI OIG, to support documented conclusions on the effectiveness of the information security program and practices of the DOI for each area evaluated.

The scope of our audit included the following:

- An inspection of relevant information security practices and policies established by the DOI OCIO as they relate to the FY2019 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 both Department and Bureau understanding of the FISMA-related policies and procedures implemented based on the guidance established by the DOI OCIO. We evaluated the policies, procedures, and practices to the applicable Federal laws and criteria to determine whether the Department and Bureaus policies, procedures and practices 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 revision 4 for our representative subset (10 %) of DOI's information systems[2]. The controls selected addressed areas covered by the DHS FY2019 Inspector General FISMA Reporting Metrics.

[2] 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 114 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/Office	Information System	CSAM ID	FIPS 199 Category
1	BIA	[redacted]	[redacted]	[redacted]
2	BLM	[redacted]	[redacted]	[redacted]
3	BOR	[redacted]	[redacted]	[redacted]
4	BSEE	[redacted]	[redacted]	[redacted]
5	FWS	[redacted]	[redacted]	[redacted]
6	NPS	[redacted]	[redacted]	[redacted]
7	OIG	[redacted]	[redacted]	[redacted]
8	OS	[redacted]	[redacted]	[redacted]
9	OSMRE	[redacted]	[redacted]	[redacted]
10	OST	[redacted]	[redacted]	[redacted]
11	USGS	[redacted]	[redacted]	[redacted]

Results of Review

Our procedures identified improvements needed in the areas of risk management, configuration management, identity and access management, and contingency planning.

The details of the weaknesses we identified are as follows.

1. Implementation of the Risk Management Program.

The table below lists findings in the risk management program.

FISMA domain	Summary of Findings
Risk Management	DOI has not consistently: • Applied security controls appropriately and effectively document the justification for not implementing selected security controls at [redacted] • Documented and approved formal configuration management policies at [redacted] • Completed remediation activities to ensure the Interagency Agreement template contains adequate language to meet the security requirements and contracting language required at [redacted] • Designed and implemented effective technical controls to detect indicators of potential attacks and prevent potential security incidents involving internal threats on the [redacted]

KPMG performed the following procedures and noted the following weaknesses in two of eleven Bureaus and Offices' risk management programs: [redacted].

[redacted]

KPMG reviewed [redacted] and determined the tailoring (applicability and justification) for security controls within control families throughout the [redacted] were not adequately evaluated. Such controls were indicated with an applicability of "Not Applicable (User determined)" and a justification that was either not relevant or not sufficient to the control.

For example, KPMG analyzed the CM control family within the [redacted] and noted that 17 of 50 controls or control enhancements were indicated as "Not Applicable (User determined)". KPMG determined 76% (13 of 17) of the controls were inadequately tailored for controls such as, but not limited to, CM-2: Baseline Configuration, CM-3: Configuration Change Control, CM-4: Security Impact Analysis, and CM-5: Access Restrictions for Change. While CM represents one of 18 control families, KPMG determined security controls throughout the [redacted] were tailored inadequately. Therefore, KPMG determined the [redacted] was not adequately documented.

KPMG inquired of management and was informed that hardware and software asset inventory procedures to support configuration management policies have not been formally documented and approved.

The [redacted] management implemented, [redacted] a tool used to collect asset inventory information and CDM scripts that are currently used on an ad-hoc basis to generate hardware and software inventories; however, these methods have not been fully deployed for asset management.

Due to the lack of tools and processes related to hardware and software inventories, KPMG determined that [redacted] management is not monitoring hardware and software inventory information and effectively reporting the results to DOI in accordance with the DOI CDM initiative.

At the request of the DOI OIG, KPMG inspected the [redacted] used for information system services with the DHS template for compliance with DOI and NIST security requirements. These templates are used when procuring services from a third party. KPMG determined the Interagency Agreement template did not contain adequate language to meet the security requirements and contracting language required for compliance with DOI and NIST standards including the protection of collecting, storing, and transporting Controlled Unclassified Information (CUI).

KPMG was unable to obtain corroborating evidence that steps outlined in the templates were executed or defined in contracting or procedural language. Without corroborating evidence, KPMG was not able to conclude that [redacted] adequately protected CUI data through contracting language in the Interagency Agreement, developed procedures that defined the steps taken to protect the data collected, or possessed supporting evidence verifying what steps were executed to protect the information.

[redacted]

KPMG inquired of the DOI management and was informed that technical controls are not in place to detect or prevent unusual network activity between Bureaus and Offices. KPMG performed tests to determine whether DOI's security controls were effective in protecting the [redacted] against internal threats, such as a malicious user with access to the DOI internal network.

The tests performed traversed the [redacted] which provides [redacted] services for the Department, Bureaus, and Offices. Over a six hour period, KPMG performed aggressive network port scans using the [redacted] tool against the [redacted] system. [redacted] is a tool generally used to gather network information, identify potential targets for further analysis, and map the network enterprise.

The DOI identified the [redacted] information system under audit as a [redacted] are assets that comprise of Federal information systems and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause significant impact to the United States' national security interests

As of October 30, 2019, our testing efforts were not reported to the [redacted] as a potential computer security incident. As these control deficiencies were identified during the audit, we brought them to the attention of the [redacted] and the [redacted] management's attention.

NIST SP 800-53, revision 4, PL-2 System Security Plan states:

The organization:

a. Develops a security plan for the information system that:

1. Is consistent with the organization's enterprise architecture;

2. Explicitly defines the authorization boundary for the system;

3. Describes the operational context of the information system in terms of missions and business processes;

4. Provides the security categorization of the information system including supporting rationale;

5. Describes the operational environment for the information system and relationships with or connections to other information systems;

6. Provides an overview of the security requirements for the system;

7. Identifies any relevant overlays, if applicable;

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];

c. Reviews the security plan for the information system [Assignment: organization-defined frequency];

d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e. Protects the security plan from unauthorized disclosure and modification.

DOI Security Control Standard, version 4.1, CM-1 Configuration Management Policy and Procedures

Applicability: All Systems

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.

DOI Security Control Standard version 4.1, CM-8 Information System Component Inventory
Control: The organization:

a. Develops and documents an inventory of information system components that:

   1. Accurately reflects the current information system;

   2. Includes all components within the authorization boundary of the information system;

   3. Is at the level of granularity deemed necessary for tracking and reporting; and

   4. Includes manufacturer, model number, serial number, software license information, system/component owner; and

b. Reviews and updates the information system component inventory *System Owner-defined frequency*.

OMB Circular NO. A-130 - Appendix I - Section (i) - Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems. Relevant excerpts include:

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 accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate);

17) Implement data-level protection and access controls to ensure the security of and access to Federal information; and

DOI Security Control Standard, System and Communications Protection, version 4.1 SC-28: Protection of Information at Rest, states:

The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].

DOI Security Control Standard, System and Communications Protection, version 4.1, dated September 2016, SC-7, Control Enhancement (21) Boundary Protection | Isolation of Information System Components | SC-7 (21) states:

The organization employs boundary protection mechanisms to separate System Owner-defined information system components supporting System Owner-defined missions and/or business functions.

DOI Security Control Standard, System and Information Integrity, version 4.1, dated September 2016, SI-4 Information System Monitoring states:

The organization:

a. Monitors the information system to detect:
    1. Attacks and indicators of potential attacks in accordance with *System Owner-defined monitoring objectives*; and,
    2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through *System Owner-defined techniques and methods;*
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and,
g. Provides *System Owner-defined information system monitoring information* to *System Owner-defined personnel or roles [Selection (one or more): as needed]; System Owner-defined frequency.*

Applicable SI-4 Information System Monitoring Control Enhancements:

(2) Information system monitoring | automated tools for real-time analysis

The organization employs automated tools to support near real-time analysis of events.

(4) Information system monitoring | inbound and outbound communications traffic

The information system monitors inbound and outbound communications traffic System Owner-defined frequency for unusual or unauthorized activities or conditions.

(5) Information system monitoring | system-generated alerts

The information system alerts System Owner-defined personnel or roles when the following indications of compromise or potential compromise occur: System Owner-defined compromise indicators.

[redacted] management did not appropriately determine the applicability of security controls and effectively document the justification for not implementing selected security controls.

[redacted] management failed to document procedures around the tools, technologies, and processes to support hardware and software asset management activities as part of Configuration Management.

[redacted] did not effectively address security requirements in the Interagency Agreement templates to ensure third party contracts and services include appropriate clauses to protect [redacted] data and information.

[redacted] have not designed, documented, and implemented effective controls to detect and report unusual network activity traversing these systems.

[redacted] Without adequately tailoring and documenting the security controls over the [redacted] system, personnel will not have an accurate view of the implementation status for security controls over the system. Without an accurate view of implementation status, the [redacted] personnel may not be able to properly perform, review, and remediate important security controls in order to maintain an effective security environment.

Without adequately defined procedures around maintaining a complete and accurate hardware and software inventory, compliance with required policies and NIST controls may not be achieved. As a result, inappropriate/unapproved or end of life hardware and software may remain on the system, resulting in systems that may be more vulnerable to attack or failure.

Without adequate security requirements and contracting language to protect data at rest in accordance with DOI policy, the bureau increases its risk exposure by not defining the accountability for each party. This could lead to security controls inadequately addressed, security incidents, improper use of controlled unclassified information, and other security issues that may cause harm to government information and information systems.

[redacted] The control deficiency, if not remediated, poses a risk to the [redacted] Management's attention and action are required to ensure that Bureau and Office's network security controls protect its network and systems against internal threats.

We recommend:

1. [redacted] review and update the [redacted] to appropriately document and tailor the security control applicability and justification statements.

2. [redacted] ensure the [redacted] document procedures for maintaining an up-to-date hardware and software asset inventory. At a minimum, the procedures should include the following elements: roles and responsibilities; technology utilized; processes followed to maintain a complete and accurate inventory; frequency with which the information system component inventory will be reviewed and updated; process to remove unauthorized, inappropriate, or end of life hardware and software from the system once identified.

3. [redacted] coordinate with DOI to design and implement a process to provide the department with CDM related information for the [redacted] system.

4. [redacted] continue to design and implement corrective actions identified in the [redacted] that addresses the protection of data at rest.

5. DOI design, document, and implement tools and technologies to monitor and detect unusual network activity from the [redacted] through the [redacted].

2. 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 consistently: • Adhered to established configuration management procedures at [redacted] • Implemented an effective patch and vulnerability management process to remediate vulnerabilities identified in vulnerability assessment scans at [redacted] • Performed monthly vulnerability scanning and has not documented monthly management procedures at [redacted] • Implemented a solution or documented procedures to monitor configuration settings and baseline configurations at [redacted] • Documented, tested, and approved security patches prior to being implemented at [redacted] • Reported [redacted] security patching information to the department in accordance with the department Continuous Diagnostics and Monitoring (CDM) initiative. • Completed the remediation of vulnerabilities identified on [redacted].

KPMG performed the following procedures and noted the following weaknesses in three of eleven Bureaus and Offices' configuration management programs: [redacted].

[redacted]

KPMG inspected the [redacted] Information Technology Configuration Management Plan and tested [redacted] change management process that included security patches. KPMG determined that [redacted] does not consistently adhere to the Bureau's established change management process, which requires changes and patches to be documented, tested, and approved prior to implementation.

KPMG obtained and inspected a population of changes made to the [redacted] information system. KPMG noted that from October 1, 2018 to August 15, 2019 there were 13 changes made to the system. KPMG judgmentally selected two system changes for inspection.

KPMG noted a deficiency in one of two system changes inspected. [redacted] was unable to provide supporting evidence over the reviewed emergency change, evidence such as request for change, the implementation plan and the roll back plan, and evidence of the system change was not discussed as part of the [redacted] meeting. Also, the emergency system change was not tested and approved in accordance with Bureau policy.

Additionally, [redacted] was not able to provide a complete listing of security patches applied to the [redacted] system, specifically [redacted], from October 1, 2018 to August 15, 2019. As such, KPMG was unable to determine whether security patches were adequately tested and approved prior to implementation.

KPMG conducted vulnerability security scans on August 14, 2019, over the [redacted] information system, [redacted] located in [redacted]. The security scans were conducted with credentialed authenticated scans utilizing [redacted]. Authenticated security scans provide more accurate test results. The [redacted] computing environment consists of [redacted] to support the application; the [redacted]. KPMG identified all [redacted] had vulnerabilities and noted that a total of 52 unique Critical, High, and Medium risk[3] [redacted] vulnerabilities were not consistently implemented in accordance with DOI Security Control Standards.

A majority of the missing security patches identified were related to [redacted] security patches such as [redacted]. Additionally, KPMG identified patches that were released by [redacted] that [redacted] did not implement; and the misconfigured [redacted] application was not remediated. Additionally, outdated [redacted] versions released back in 2017 were primarily identified on the [redacted]. Moreover, KPMG noted that the servers had weak encryption settings to include weak [redacted] encryption and untrusted certificates. [redacted] and [redacted] are protocols that provide authentication and data encryption between servers, applications, and workstations.

KPMG informed [redacted] of the vulnerabilities described above and provided detailed results from our testing. KPMG noted that the vulnerability is on the host server, and therefore other applications on that server are impacted. KPMG was further informed that the [redacted] configuration is going through an upgrade process and is estimated to be completed by September 30, 2019; however, as of October 4, 2019, KPMG was unable to confirm the extent of the remediation.

[redacted]

There are no documented procedures to perform monthly vulnerability scanning for the [redacted] and [redacted] has not fully implemented a [redacted] compliant tool to perform vulnerability scanning activities. Management is currently performing vulnerability assessment activities annually using manual scripts to identify system vulnerabilities.

Additionally, [redacted] does not have procedures in place to support configuration baseline monitoring and [redacted] has not implemented a solution to monitor configuration settings and baseline configurations.

Due to the lack of tools and processes related to configuration baseline monitoring and vulnerability scanning, KPMG determined that [redacted] is not monitoring vulnerability and configuration management information, nor effectively reporting the results to DOI in accordance with the DOI CDM initiative.

KPMG inspected the [redacted] patch management documentation and determined [redacted] management is operating the program on an ad-hoc basis. As software or operating system changes are identified, management performs a system check to determine whether the system requires security patches to be implemented.

[3] Risk ratings were determined by [redacted] tool.

[4] [redacted] contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue. [redacted] has published [redacted] plugins, covering [redacted] and [redacted] is a reference-method for publically known information-security vulnerabilities and exposures. [redacted] is an electronic mailing list dedicated to issues about computer security.

Also, management has not implemented a comprehensive program to monitor the [redacted] system components for compliance with patch and configuration management practices.

KPMG noted that management implemented 77 security patches during the period of October 1, 2018 to June 14, 2019. KPMG noted that management was unable to provide documentation validating that 15 of 15 security patches sampled were not formally documented, tested, and approved prior to being implemented.

KPMG determined that that [redacted] patching program is deficient and the system is not reporting patching information to DOI in accordance with DOI CDM initiative.

[redacted]

KPMG conducted internal vulnerability security scans on August 19, 2019, over the [redacted] information system, [redacted] located in [redacted] The security scans were conducted with credentialed authenticated privileges utilizing [redacted]. Authenticated security scans provide more accurate test results. The [redacted] computing environment consists of [redacted] servers to support the application; [redacted] servers and [redacted] server. In addition, KPMG conducted an external non-credentialed vulnerability scan over the publicly available portion of the [redacted]

KPMG identified 84 unique Critical, High, and Medium risk[5] [redacted] vulnerabilities across all [redacted] devices scanned, which were not consistently remediated in accordance with DOI IT Security Control Standards. The majority of the vulnerabilities identified were related to [redacted] security patches such as [redacted] with the oldest patch released in 2010.

Additionally, KPMG identified [redacted] updates that were released in 2010, and [redacted] patches released in 2017. Moreover, KPMG noted that the servers had weak encryption settings to include weak [redacted] encryption and untrusted certificates. [redacted] and [redacted] are protocols that provide authentication and data encryption between servers, applications, and workstations.

KPMG informed the [redacted] of the vulnerabilities described above and provided detailed results for testing. [redacted] management took immediate action when notified of the security weaknesses and created two [redacted] Additionally, KPMG was informed that [redacted] server was remediated by decommissioning the server through the change control ticketing process [redacted] and management provided evidence that remediation efforts were ongoing for the remaining [redacted] servers around the items noted during our testing period. KPMG was unable to confirm the extent of the remaining remediation.

[redacted] Information Technology Configuration Management Program Configuration Management Plan, version 1.1, Section 4.5.3 Emergency Change

Emergency Changes are changes intended to repair an error in an IT service that is negatively impacting the business to a high degree, for example to resolve a Major Incident or implement a Security patch and must be introduced as soon as possible.

[5] Risk ratings were determined by [redacted] tool.

[6] [redacted] contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue. [redacted] has published [redacted], covering [redacted] is a reference-method for publically known information-security vulnerabilities and exposures. [redacted] is an electronic mailing list dedicated to issues about computer security.

As much testing, as possible of the Emergency Change should be carried out. Consideration should be given to how much it would cost to fully test the change with the Change failing factored by the anticipated likely hood of its failure. Implementing completely untested changes should be avoided, if a Change goes wrong, the cost is usually greater than that of adequate testing.

All Emergency Changes must be documented in accordance with Change Management policies, though such documentation need not be submitted or completed prior to change implementation.

Emergency Changes are processed through the [redacted]

NOTE: Changes intended to introduce immediately required business improvements (Emergency Releases) are handled as Normal Changes, assessed as having the highest urgency.

[redacted]

revision 2.1, 3.1 Major Changes

Major Changes: Significant changes that affect the functionality, security controls, or baseline configurations of the [redacted]

Major changes are:

- Application of security patches
- Operating system upgrades/service packs
- Revisions to software code
- Database updates
- Display screen updates
- Changes to function ability or security settings of third-party software or firmware
- Updating procedures and job plans from "dot" revisions to final approved revisions.

Major changes would also include the removal or replacement of [redacted] In addition, any changes that do not have an approved procedure are considered a major change. When available, approved procedures for significant changes allow the work to be performed without prior board approval. All major changes must have any applicable [redacted] reviewed and updated as part of the initial change assessment process.

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

Applicability: All Information Systems

Control: The Organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within System Owner-defined time period, not to exceed thirty days, of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

DOI Security Control Standards Configuration Management, version 4.1, CM-3 Configuration Change Control states: The Organization:

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

DOI Security Control Standard, Risk Assessment, version 4.1, dated September 2016, RA-5 Vulnerability Scanning: The organization:

a. Scans for vulnerabilities in the information system and hosted applications *System Owner-defined frequency and/or randomly in accordance with organization-defined process, but at least monthly,* and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities within thirty days for high-risk vulnerabilities; within ninety days for moderate risk vulnerabilities in accordance with an organizational assessment of risk; and,
e. Shares information obtained from the vulnerability scanning process and security control assessments with *System Owner-defined personnel or roles* to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

DOI Security Control Standard, Identification and Authentication, version 4.1, dated September 2016, IA-5 Authenticator Management states: The organization manages information system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators at least every 60 days, unless specified and allowed to be greater by DOI or NIST National Vulnerability Database (NVD) security configuration checklists and profiles specific to mobile devices (e.g., device authenticators for Portable Electronic Devices and Personal Digital Assistants (PEDs/PDAs), Tablet PCs, Smartphones or other mobile embedded devices), but not greater than 90 days;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

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

Applicability: All Information Systems

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.

[redacted] did not enforce its established configuration management plan that requires testing and approvals of implemented changes be documented and maintained. [redacted] has not defined a process to identify all security patches implemented on the [redacted] system.

[redacted] and the Department recently transitioned to [redacted] as the enterprise solution to vulnerability [redacted] replacing the previously utilized tool, [redacted] Due to this transition, [redacted] has not implemented effective controls to patches for known vulnerabilities as they were not properly identified in a timely manner and patches were not consistently implemented in order to meet the remediation timeframe.

[redacted] management did not prioritize the development and implementation of controls to meet DOI Security Control Standards and NIST SP 800-53, revision 4 requirements for CM-06 and RA-05.
[redacted] management did not implement a comprehensive security patch management program that monitors [redacted] endpoints for security patching compliance ensuring that patches are applied timely to meet DOI policy.

Additionally, [redacted] management is not enforcing its established configuration management plan that requires testing and approvals of implemented security patches be documented and retained.

[redacted] The Department recently transitioned to [redacted] as the [redacted] replacing the previously utilized tool, [redacted] Furthermore, due to the manual process of patching the [redacted] systems, management has difficulty in comprehensively implementing security patches within the designated timeline for critical, high, and medium risk vulnerabilities.

[redacted] Critical errors, system compromises and disruption of servicers could occur if system changes are not tested and approved and the change process is not followed, documented and retained as required.
Inconsistent patch management and system configurations can lead to increased risk to the [redacted] computing environment, which is vital to [redacted] mission. The organizational risks could lead to potential inappropriate system access, system errors, and potential lost or disclosure of [redacted] information.

[redacted] Without adequate vulnerability scanning and configuration baseline monitoring procedures and tools in place, [redacted] cannot ensure the cybersecurity hygiene and compliance of the [redacted] network infrastructure. The lack of proper vulnerability scanning and configuration monitoring capabilities could put high-value assets and information at risk of compromise and/or failure. Critical errors, system compromises and disruption of servicers could occur if security patches are not implemented timely and the patch process is not followed, documented and retained as required.

[redacted] Inconsistent patch management and system configurations can lead to increased risk to the [redacted] computing environment, which is vital to the [redacted] mission. The organizational risks could lead to potential inappropriate system access, system errors, and potential lost or disclosure of [redacted] information.

We recommend [redacted]

6. Enforce the established [redacted] configuration management plan that requires emergency changes, including security patches, to be documented, tested, and approved through the [redacted] change management process.

7. Design and implement a process for identifying all security patches applied to the [redacted] servers.

8. Enhance oversight compliance to ensure all relevant and appropriate system security patches are applied timely in order to effectively implement patches as required. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.

9. Develop a solution for the [redacted] utilizing proper encryption mechanisms, such as [redacted] disabling of [redacted] and renewal of the proper certificate.

We recommend [redacted] document and implement:

10. Procedures that require vulnerability scanning of [redacted] to be performed at least [redacted]
11. A solution that will provide the [redacted] with the functionality to perform vulnerability scanning across all components.
12. Procedures that require baseline configurations to be developed, documented, and monitored for compliance.
13. A solution that will provide the [redacted] with the functionality to perform configuration baseline monitoring for baseline compliance.
14. Implement recommendation #3 noted on page 15 in this report.
15. Processes and technology that will support a security patching program that monitors [redacted] endpoints for security patching version compliance and ensures that patches are applied timely to meet DOI Security Control Standard Risk Assessment, V4.1, control RA-5.
16. Enforcement of established [redacted] patch implementation procedures that requires security patches be documented, tested, and approved through the [redacted] change management process.
17. Implement recommendation #3 noted on page 15 in this report.

We recommend [redacted]

18. Ensure that the [redacted] is properly configured to perform credentialed vulnerability scanning on all [redacted] assets.

19. Enhance oversight compliance to ensure all relevant and appropriate system security patches for [redacted] are applied timely in order to effectively implement patches as required. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation within a [redacted].

3. 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 consistently: • Implemented a formal user access authorization process for non-privileged users at the [redacted] • Reviewed system audit logs for unusual activity at [redacted] • Implemented an effective user account management review process at [redacted] • Implemented personnel screening procedures at [redacted]

KPMG performed the following procedures and noted the weaknesses in two of eleven Bureaus and Offices' identity and access management programs: [redacted].

[redacted]

KPMG inquired of [redacted] management and was informed that the [redacted] does not have a formal user access authorization process in place for non-privileged users. In addition, KPMG obtained and inspected the [redacted] Procedures, dated May 20, 2016, revision 4 and determined that a formal access authorization process is in place for privileged users; however, the process [redacted] has approximately [redacted] non-privileged users.

[redacted]

KPMG inquired of [redacted] management and was informed that the [redacted] which includes the [redacted] information system under audit, has enabled audit logs that capture user logins and user actions performed by privileged users, such as system administrators. However, KPMG was informed that the [redacted]

KPMG was informed that the user access review was completed on July 15, 2019; however the review did not include whether user accounts were valid and user permissions were appropriate. The review was limited to the inspection of last login date for users. Users with a last login of more than a year prior were contacted to ask if the access was still needed. If the user indicated that access was no longer needed or did not reply, access was removed.

KPMG inquired of management and inspected the [redacted] user list and noted a population of [redacted] active users, [redacted] of which had new access provisioned during the audit period. KPMG randomly selected a sample of 15 [redacted] new users and inspected evidence of their Position Descriptions (PDs), Position Risk Designation Records (PDRs), and Background Investigations. KPMG noted the following deficiencies:

- Four of 15 sampled users did not have a PDR retained.
- Three of four sampled users noted above did not have a PD retained.
- As of September 6, 2019, [redacted] was unable to provide evidence of a background investigation was performed for 10 of 15 selected users.

DOI Security Control Standards Personnel Security, version 4.1, AC-2 Account Management

Control: The organization:

a. Identifies and selects the following types of information system accounts to support organizational missions/business functions (i.e., individual, group, system, application, guest/anonymous, and temporary);
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by organizational account managers for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with *System Owner-defined procedures or conditions*;
g. Monitors the use of, information system accounts;
h. Notifies account managers:
    1. When accounts are no longer required;
    2. When users are terminated or transferred; and
    3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements at least annually; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

DOI Security Control Standards Personnel Security, version 4.1, AC-6 Least Privilege
Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

DOI Security Control Standard Access Control, version 4.1, AC-6 (9) Least Privilege | Auditing Use of Privileged Functions

The information system audits the execution of privileged functions.

DOI Security Control Standard Access Control, version 4.1, AU-6 Audit Review, Analysis, And Reporting
Control: The organization:

a. Reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity; and

b. Reports findings to designated organizational officials.

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

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

[redacted]

[redacted] limited the access review over the [redacted] information system to a search for [redacted] and did not validate all user accounts or inspect access roles for appropriateness. [redacted] did not effectively implement a comprehensive position risk determination process to include maintaining position descriptions and position designation records.

[redacted] Without a formal user access authorization process, to include the request and approval of user access, the risk of unauthorized access to the [redacted] information system increases.

[redacted] Not auditing privileged functions on a [redacted] basis increases the risk of undetected inappropriate and/or unauthorized activity in the system, which can potentially lead to significant adverse impacts including data integrity and the general health of the information system.

User access reviews are designed to ensure every account is valid and access roles/permissions are appropriate. By not performing these tasks for the [redacted] information system, the integrity and confidentiality of the data within the system could be compromised, potentially leading to incorrect information being provided to stakeholders as it relates to the storage, retrieval, and dissemination of case information supporting land, mineral status and use authorizations.

PDs, PDRs, and background investigations are essential documents to an effective personnel screening program. When such documents cannot be located, challenges arise in ensuring documents are reviewed at the required frequencies and performed correctly. As a result, personnel may have out of date or incorrect background investigations for their positions, which could compromise the security and integrity of data within the [redacted] system and the [redacted]

We recommend:

20. [redacted] define and document a formal process for [redacted] to include the request and approval for [redacted].
21. [redacted] document and implement a formal process for [redacted].
22. [redacted] ensure all [redacted] users, roles, and permissions are reviewed at least [redacted] to ensure access is restricted to appropriate personnel who require the access for their job duties.
23. [redacted] enhance the position risk designation process to ensure all position descriptions, position designation records, and background investigations for positions and personnel are maintained and available for review.

4. Implementation of the Contingency Plan program.

The table below lists findings in the contingency plan program.

FISMA Domain	Summary of Findings
Contingency Plan	DOI has not consistently: • Reviewed and updated information system contingency plans at [redacted] • Ensured business impact analysis templates meet federal requirements at [redacted] and [redacted] • Conducted functional contingency plan tests or exercises, nor documented results for moderate impact information systems at [redacted].

KPMG performed the following procedures and noted the following weaknesses in three of eleven Bureaus and Offices' contingency plan programs: [redacted].

[redacted]

KPMG inspected the [redacted] dated [redacted] 2017, and noted the [redacted] lists the [redacted] for the mission/business processes and the servers that support [redacted] KPMG compared the [redacted] recovery time objectives to the [redacted] contingency plan and determined the [redacted] contingency plan did not align with the [redacted] requirements established by its current [redacted]

KPMG reviewed the [redacted] Contingency Plan tabletop exercise results, dated [redacted]/2019, and inquired of management and was informed that the [redacted], which supports the [redacted], did not completely perform a contingency plan test or exercise to include a functional test. [redacted] performed a tabletop exercise that reviewed through the roles, responsibilities, and processes of a simulated contingency event.

[redacted]

KPMG obtained and inspected the [redacted] and determined that the [redacted] did not include the identification of system resource requirements or the of recovery time priority for the [redacted]. KPMG noted that the standard [redacted] template was used for the [redacted]. KPMG further determined that the [redacted] template did not include the identification of resource requirements and the identification of recovery priorities for system resources; both key components of a [redacted] per NIST SP 800-34, revision 1.

[redacted]

KPMG obtained and inspected results from the Incident Response Plan/Contingency Plan Exercise conducted on [redacted] 2019 and noted the [redacted] which includes the [redacted] was tested with a table top exercise. However, the [redacted] is a moderate impact system which requires a functional CP test.

NIST SP 800-53, revision 4, CP-2: Contingency Plan

The organization:

A. Develops a contingency plan for the information system that:
    a. Identifies essential missions and business functions and associated contingency requirements;
    b. Provides recovery objectives, restoration priorities, and metrics;
    c. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
    e. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    f. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
B. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
C. Coordinates contingency planning activities with incident handling activities;
D. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];
E. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
F. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
G. Protects the contingency plan from unauthorized disclosure and modification.

DOI Security Control Standard Contingency Planning, version 4.1, CP-4 Contingency Plan Testing

Applicability: All Systems

Control: The organization:

a. Tests the contingency plan for the information system at least annually using functional exercises for moderate impact systems; classroom exercises/tabletop written tests for low impact systems to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

NIST SP 800-34, revision 1, Contingency Planning Guide for Federal Information Systems

Relevant excerpts from NIST guidance:

Three steps are typically involved in accomplishing the Business Impact Assessment:

1. Determine mission/business processes and recovery criticality. Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.

2. Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as 14 NIST SP 800-37 further describes the RMF and provides guidance on organization-wide risk management including the development of risk management strategies, risk-related governance issues, defining protection requirements and associated risks for organizational mission/business processes, integration of security and privacy requirements into enterprise architectures, and managing risk within the system development life cycle. CHAPTER 3 15 CONTINGENCY PLANNING GUIDE FOR FEDERAL INFORMATION SYSTEMS quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

[redacted] management did not incorporate the [redacted] results from the [redacted] business impact analysis into the [redacted] contingency plan.

[redacted] failed to ensure the DOI Security Control Standard for Contingency Plan Testing (CP-4) was adequately tested for the [redacted].

[redacted] Management did not design the [redacted] identify system resource requirements or to identify recovery priorities for system resources.

[redacted] management did not account for the system's FIPS 199 Security Categorization of moderate when conducting the system's annual CP test.

[redacted] In the event the [redacted] is activated to recover the [redacted] system, which have a tolerable downtime of no longer than [redacted], would not be available for as long as [redacted]. This could potentially cause loss of mission critical services for a period that is significantly longer than what is deemed appropriate by the [redacted] business impact assessment, resulting in an impact to the US national security.

Without performing a functional exercise of the contingency plan, there is an increased risk of a significant disruption in services provided by the [redacted] system, which could potentially lead to loss of data, inability to collect data, and inability to perform mission critical functions for the bureau, in the event of a disaster.

[redacted] Using [redacted], which does not define the system resources that support the business functions and the associated recovery time objectives to restore those resources, [redacted] may not be able to adequately recover critical resources in a timely manner, which impacts [redacted] ability to restore critical business functions that support the mission of [redacted]

[redacted] The [redacted] test may not adequately assess the effectiveness of the system's CP. As a result, the [redacted] may not be adequate to ensure continued essential [redacted] activities in the event of a critical failure or occurrence requiring the initiation of the CP.

We recommend:

24. [redacted] review and update the [redacted] contingency plan and consider the [redacted] for [redacted] and other information systems that inherit contingency plan controls from the [redacted].

25. [redacted] enforce the requirements outlined in the DOI Security Control Standards for Contingency Planning and ensure contingency plan tests for moderate impact systems include a functional test and results are documented.

26. [redacted] management ensure their [redacted] template aligns with the NIST SP 800-34, revision 1 key components for a [redacted].

27. [redacted] test the [redacted] in accordance with NIST requirements and DOI Security Control Standards using a functional test for the [redacted] moderate system.

Conclusion

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

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

JAN 1 5 2020

Memorandum

To: Mark Lee Greenblatt, Inspector General

From: William E. Vajda, Chief Information Officer

Subject: Management Response to the Federal Information Security Modernization Act of 2014 (FISMA) Revised Draft Fiscal Year 2019 Performance Audit Report 2019-ITA-034 (Report)

Thank you for the opportunity to review and respond to the December 20, 2019 revised draft FISMA Report. The Office of the Chief Information Officer (OCIO) concurs with the Report recommendations. The OCIO notes that bureaus and offices had already commented on individual Notice of Findings and Recommendations" before issuance of this draft report. Those comments are included as bureau and office "Management Response to Report" on pages 32-35 of this Report.

OCIO is providing a coordinated Departmental response with Corrective Action Plans (CAPs) and Target Completion dates as Attachment 1.

If you have questions, please contact me at (202) [redacted]. Staff may contact Jack Donnelly, Chief Information Security Officer, at (202) [redacted].

Attachment 1: The Department of the Interior's Management Response to the Fiscal Year 2019 Revised Draft OIG FISMA Performance Audit Report 2019-ITA-034

Cc

Tonya R. Johnson, Deputy Chief Financial Officer and Director Office of Financial Management
Nancy Thomas, Acting Division Chief, Internal Control and Audit Follow-up, Office of Financial Management
KPMG LLP, 8350 Broad St, Mclean, VA 22102
Richard Westmark, Chief, OCIO Compliance and Audit Management
Morgan Aronson, Director, Financial Audits, Office of Inspector General
Marleah Domergue, Headquarter Operations, Office of Inspector General

Attachment 1:

The Department of the Interior's Management Response to the Fiscal Year 2019 Draft OIG FISMA Performance Audit Report, 2019-ITA-034

Please find the Department of the Interior's (DOI) management responses to the 27 recommendations from the Report below:

Recommendation 1. [redacted] review and update the [redacted] to appropriately document and tailor the security control applicability and justification statements.

Management Response: Concur. [redacted] has been created to address this recommendation. Security controls that are currently tailored as not applicable will be reviewed and re-tailored as appropriate. [redacted] will monitor correction actions via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 2. [redacted] ensure the [redacted] document procedures for maintaining an up-to- date hardware and software asset inventory. At a minimum, the procedures should include the following elements: roles and responsibilities; technology utilized; processes followed to maintain a complete and accurate inventory; frequency with which the information system component inventory will be reviewed and updated; process to remove unauthorized, inappropriate, or end of life hardware and software from the system once identified.

Management Response: Concur. [redacted]. CM-01 policy components will be inherited from DOI if applicable, and required procedures will be developed around maintaining an up-to-date hardware and software asset inventory. [redacted] will monitor correction actions via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 3. [redacted] coordinate with DOI to design and implement a process to provide the department with CDM related information for the [redacted] system.

Management Response: [redacted] management will address this recommendation with a risk acceptance via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 1/10/2020

Recommendation 4. [redacted] continue to design and implement corrective actions identified in the [redacted] that addresses the protection of data at rest.

Management Response: Concur. [redacted] concurs if the scope of the finding is just to complete the corrective actions identified in [redacted], opened as a result of 2018-[redacted] in accordance with OCIO Directive_2019-00, [redacted] already has a policy in place that states that only [redacted] (focus of identified cause) with FIPS 140-2 compliant encryption will be approved. (IMT Circular 18-01 and IMT Item List). [redacted] will monitor correction actions via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 10/30/2020

Recommendation 5. DOI Design, document, and implement tools and technologies to monitor and detect unusual network activity from the [redacted] through the [redacted] to the [redacted].

Management Response: Concur. The [redacted] will review the monitoring of their system. OCIO will review the conditions and recommendations pertaining to the specified Controls and provide guidance as needed to [redacted] will track its action via [redacted]. OCIO will tracking its action via [redacted]

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020.

Recommendation 6. [redacted] enforce the established [redacted] configuration management plan that requires emergency changes, including security patches, to be documented, tested, and approved through the [redacted] change management process.

Management Response: Concur. [redacted] will enforce the established [redacted] configuration management plan for emergency changes. [redacted] will monitor its implementation via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 7. [redacted] design and implement a process for identifying all security patches applied to the [redacted] servers.

Management Response: Concur. [redacted] will design and implement a process for identifying all security patches applied to the [redacted] will monitor its implementation via [redacted]

Responsible Official(s): [redacted].

Target Date of Completion: 12/31/2020

Recommendation 8. [redacted] enhance oversight compliance to ensure all relevant and appropriate system security patches are applied timely in order to effectively implement patches as required. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.

Management Response: Concur. [redacted] will enhance oversight compliance to ensure relevant security patches are applied to [redacted] will monitor its implementation via 38441.

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 9. [redacted] develop a solution for the [redacted] web server utilizing proper encryption mechanisms, such as [redacted], disabling of [redacted] and renewal of the proper certificate.

Management Response: Concur. [redacted] will develop a solution for [redacted] to utilize proper encryption mechanisms. [redacted] will monitor its implementation via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 10. [redacted] document and implement procedures that require vulnerability scanning of [redacted] to be performed at least [redacted]

Management Response: Concur. [redacted] opened on 6/28/2019. Remediation will ensure vulnerability scanning occurs across components that can withstand the activity without negative impacts. [redacted] will monitor correction actions via [redacted]
Responsible Official(s): [redacted]
Target Date of Completion: 12/31/2020

Recommendation 11. [redacted] document and implement a solution that will provide the [redacted] with the functionality to perform vulnerability scanning across all components.

Management Response: Concur. [redacted] opened on 6/28/2019. Remediation will ensure vulnerability scanning occurs across components that can withstand the activity without negative impacts. [redacted] will monitor correction actions via [redacted].
Responsible Official(s): [redacted]
Target Date of Completion: 12/31/2020

Recommendation 12. [redacted] document and implement procedures that require baseline configurations to be developed, documented, and monitored for compliance.

Management Response: Concur. [redacted] opened on 7/12/2019. Remediation will ensure that baseline configurations are developed, documented and monitored for compliance. [redacted] will monitor correction actions via [redacted]
Responsible Official(s): [redacted]
Target Date of Completion: 12/31/2020

Recommendation 13. [redacted] document and implement a solution that will provide the [redacted] with the functionality to perform configuration baseline monitoring for baseline compliance.

Management Response: Concur. [redacted] opened on 7/12/2019. Remediation will ensure that baseline configurations are monitored for compliance. [redacted] will monitor correction actions via [redacted].
Responsible Official(s): [redacted]
Target Date of Completion: 12/31/2020

Recommendation 14. [redacted] implement recommendation #3 noted above in this report. Management Response: Same as that for Rec. #3.

Recommendation 15. [redacted] document and implement processes and technology that will support a security patching program that monitors [redacted] endpoints for security patching version compliance and ensures that patches are applied timely to meet DOI Security Control Standard Risk Assessment, V4.1, control RA-5.

Management Response: Concur. [redacted] opened on 6/28/2019. Remediation will ensure that patches are consistently applied within [redacted] or a Risk Based Decision to follow the NERC CIP timelines, instead of the FISMA requirements, will be approved if adequate justification and compensating controls exist. [redacted] will monitor correction actions via [redacted]
Responsible Official(s): [redacted]
Target Date of Completion: 12/31/2020

Recommendation 16. [redacted] enforce established [redacted] patch implementation procedures that requires security patches be documented, tested, and approved through the [redacted] change management process.

Management Response: Concur. [redacted] opened on 6/28/2019. Remediation will ensure that the Change Control Procedures related to patching requirements are reviewed, updated if necessary, and consistently followed. [redacted] will monitor correction actions via [redacted]

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 17. [redacted] implement recommendation #3 noted above in this report. Management Response: Same as that for Rec. #3.

Recommendation 18. [redacted] ensure that the [redacted] is properly configured to perform credentialed vulnerability scanning on all [redacted].

Management Response: Concur. We will ensure [redacted] is properly configured for all [redacted] assets. We have opened [redacted] to address the remaining mitigations that we will monitor and provide resolution.

Responsible Official(s): [redacted] Target Date of Completion: 12/31/2020

Recommendation 19. [redacted] enhance oversight compliance to ensure all relevant and appropriate system security patches are applied timely in order to effectively implement patches as required. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation within a POAM.

Management Response: Concur. We will ensure oversight procedures for [redacted] reporting are properly updated for all [redacted] assets. We have opened [redacted] to address the remaining mitigations that we will monitor and provide resolution.

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 20. [redacted] define and document a formal process for authorizing non- privileged user access to include the request and approval for user access to [redacted]

Management Response: Concur. [redacted] will define and document the [redacted] user access to include 1. User review (grandfathered existing users) 2. Use of a Webforms form for authorization [redacted] approval process is in production. [redacted] will monitor the corrective actions via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 21. [redacted] document and implement a formal process for reviewing the audit logs for potential misuse of privileged functions and actions.

Management Response: Concur. [redacted] will document and implement a formal process for reviewing [redacted] for potential misuse of privileged functions and actions. [redacted] will monitor the corrective actions [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 22. [redacted] ensure all [redacted] users, roles, and permissions are reviewed at least annually to ensure access is restricted to appropriate personnel who require the access for their job duties.

Management Response: Concur. [redacted] will review active and non-active [redacted] user accounts to restrict access to appropriate personnel. [redacted] will monitor the corrective actions [redacted]

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 23. [redacted] enhance the position risk designation process to ensure all position descriptions, position designation records, and background investigations for positions and personnel are maintained and available for review.

Management Response: Concur. [redacted] will enhance the position risk designation process to ensure position descriptions, position designation records, and background investigations for positions and personnel are maintained and available for review within the timeframe identified in policy. [redacted] will monitor the corrective actions [redacted].

Responsible Official(s): [redacted].

Target Date of Completion: 12/31/2020

Recommendation 24. [redacted] review and update the [redacted] contingency plan and consider the [redacted] for [redacted] and other information systems that inherit contingency plan controls from the [redacted].

Management Response: Concur. [redacted] will review and update the [redacted] contingency plan and consider the [redacted] will monitor the corrective actions via [redacted]

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 25. [redacted] enforce the requirements outlined in the DOI Security Control Standards for Contingency Planning and ensure contingency plan tests for moderate impact systems include a functional test and results are documented.

Management Response: Concur. [redacted] will implement requirements for CP-4 Contingency Planning Testing in accordance with the categorization of the system. [redacted] will monitor the corrective actions via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

Recommendation 26. [redacted] management ensure their [redacted] template aligns with the NIST [redacted], Revision 1 key components for a [redacted]

Management Response: Implemented. [redacted] corrected the deficiency while KPMG was on site. After reviewing [redacted], Revision 1, Appendices, The [redacted] template was updated to align with [redacted] on 9/5/2019.

Recommendation 27. [redacted] test the [redacted] in accordance with NIST requirements and DOI Security Control Standards using a functional test for the [redacted] moderate system.

Management Response: Concur. [redacted] was opened on 9/16/2019.

Remediation will ensure that the Contingency Plan undergoes a functional test in accordance with NIST requirements and DOI Security Control Standards as a moderate system. [redacted] will monitor correction actions via [redacted].

Responsible Official(s): [redacted]

Target Date of Completion: 12/31/2020

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 FY2019 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.

Table: Cybersecurity Framework Control Deficiencies Identified, by Organization, by Function

Functions	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			X					X			
[redacted]		X	X					X			X
[redacted]											
[redacted]											
[redacted]		X	X							X	

Legend: X – Weakness identified in Cybersecurity function

Appendix II – Listing of Acronyms

Acronym	Definition
AICPA	American Institute of Certified Public Accounts
AC	Access Control
ACF	Adobe Cold Fusion
ACIO	Associate Chief Information Officer
ACISO	Associate Chief Information Security Officer
ASOC	Advanced Security Operations Center
AU	Audit and Accountability
BIA	Bureau of Indian Affairs
[redacted]	[redacted]
[redacted]	[redacted]
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
CA	Security Assessment and Authorization
CDM	Continuous Diagnostics and Mitigation
[redacted]	[redacted]
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CR	Change Request
[redacted]	[redacted]
CSAM	Cyber Security Assessment and Management
CUI	Controlled Unclassified Information

CVE	Common Vulnerability and Exposures
DHS	Department of Homeland Security
DOI	United States Department of the Interior
[redacted]	[redacted]
[redacted]	[redacted]
EODS	Entrance On Duty System
ESN	Enterprise Services Network
[redacted]	[redacted]
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FWS	US Fish and Wildlife Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
IA	Identification and Authentication
IA	Information Assurance
IAM	Identity and Access Management
ICS	Industrial Control System
ID	Identifier
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
IT	Information Technology
KPMG	KPMG LLP
LAN	Local Area Network
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
[redacted]	[redacted]
NPS	National Park Service
[redacted]	[redacted]
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
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
PD	Position Description
PDR	Position Risk Designation Record
PIV	Personal Identity Verification
PL	Planning
POA&M	Plan of Action and Milestones
PUB	Publication
RA	Risk Assessment
REV	Revision
RFQ	Request for Quotation
[redacted]	[redacted]
RM	Risk Management
[redacted]	[redacted]
SA	System and Services Acquisition
SC	System and Communication Protection

[redacted]	[redacted]
SI	System and Information Integrity
SP	Special Publication
[redacted]	[redacted]
SSP	System Security Plan
ST	Security and Awareness Training
[redacted]	[redacted]
US	United States
USC	United States Code
USGS	United States Geological Survey
[redacted]	[redacted]

Appendix III – Prior Year Recommendation Status

Below is a summary table of the [redacted] FISMA report recommendations and the status as of October 31, 2019.

Table 1 [redacted] FISMA Report Recommendations and Status as of October 31, 2019.
11 of 18 Recommendations are Open

Description	Status
1. [redacted]	Open. Target Completion Date: [redacted]
2. [redacted]	Open. Target Completion Date: [redacted]
3. [redacted]	Closed.
4. [redacted]	Closed.
5. [redacted]	Open. Target Completion Date: [redacted]
6. [redacted]	Closed.
7. [redacted] [redacted] b. [redacted]	Closed.

8. [redacted]	Closed.
9. [redacted]	Closed.
10. [redacted]	Open. Target Completion Date: [redacted]
11. [redacted]	Open. Target Completion Date: [redacted]
12. [redacted]	Open. Target Completion Date: [redacted]
13. [redacted]	Closed.
14. [redacted]	Open. Target Completion Dates: [redacted]
15. [redacted]	Open. Target Completion Date: [redacted]
16. [redacted]	Open. Target Completion Date: [redacted]

17. [redacted]	Open. Target Completion Date: [redacted]
18. [redacted]	Open. Target Completion Date: [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 2019 Questions for Inspectors General

The information included represents the Department of the Interior (DOI) responses to Department of Homeland Security's (DHS) FISMA 2019 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 2019 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 2019 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: Based on results of testing, the maturity level was assessed as Consistently Implemented (Level 3), which is not effective.

- Risk Management – Consistently Implemented (Level 3)
- Configuration Management – Consistently Implemented (Level 3)
- Identity and Access Management – Managed and Measurable (Level 4)
- Data Protection and Privacy – Consistently Implemented (Level 3)
- Security Training – Managed and Measurable (Level 4)
- Information System Continuous Monitoring – Managed and Measurable (Level 4)
- Incident Response – Consistently Implemented (Level 3)
- Contingency Planning - Consistently Implemented (Level 3)

A Performance Audit was performed over the information security program of the Department of the Interior (DOI) to determine the effectiveness of such program for the fiscal year ending September 30, 2019. 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 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 114 operational unclassified information systems and 11 information systems were randomly selected for the audit.

Consistent with applicable FISMA requirements, OMB policy, and NIST standards, 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 effective as weaknesses were identified three of five function areas, Identify, Respond, and Recover. The Protect and Detect function areas were effective.

Weaknesses were noted in the FISMA domain areas of risk management, configuration management, data protection and privacy, incident response, and contingency planning metric domains. Consistent with the Fiscal Year (FY) 2019 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 and Detect functions at Managed and Measurable (Level 4). The Identify, Recover, and Respond functions were assessed at Consistently Implemented (Level 3). Overall, DOI was assessed at Consistently Implemented (Level 3).

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. Rev. 4: CA-3, PM-5, and CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

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.

Department of the Interior (DOI) maintains an inventory of its information systems in the Cyber Security Assessment and Management (CSAM) risk management tool. CSAM 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 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).

Maturity Level: Managed and Measurable (Level 4) - The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and 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 Rev. 4: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?

Maturity Level: Managed and Measurable (Level 4) – The organization ensures that the software assets on the network (and their associated licenses) are covered by an organization-wide software asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.

10 of 11 [redacted] utilize 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 Continuous Diagnostics and Mitigation (CDM) software solution as part of their software asset management suite of tools. [redacted] did not define and implement a process for maintaining a current software inventory for one information system that is not connected to the DOI network.

DOI can improve and increase its maturity level by fully implementing an organization-wide software asset management capability.

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Maturity Level: Optimized (Level 5) – The organization utilizes impact-level prioritization for additional granularity to support risk-based decision-making.

DOI has consistently defined its mission and business functions in risk management policies and procedures and implemented the NIST Risk Management Framework. DOI maintains a prioritized inventory of high value assets that is reviewed at least annually. All information systems to include high value assets are assigned a Federal Information Processing Standard (FIPS) 199 impact rating.

5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This 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 Rev. 4: 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; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 – 2; SECURE Technology Act: s. 1326)?

Maturity Level: Ad Hoc (Level 1). The organization has performed an organization-wide security and privacy risk assessment. Risk management policies, procedures, and strategy have been developed and communicated across the organization. The strategy clearly states risk management objectives in specific and measurable terms. As appropriate, the organization has developed an action plan and outlined its processes to address the supply chain risk management strategy and related policy and procedural requirements of the SECURE Technology Act.

DOI has established and implemented its risk management policies and procedures across the enterprise. However, DOI has not designed a formal action plan for establishing a supply chain risk management program in accordance with the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE). Existing supply chain risk management practices are in place that address IT supply chain risk management and DOI intends to incorporate the practices into other cybersecurity risk management activities.

DOI can improve and increase its maturity level by formally developing and implementing an action plan to address the supply chain risk management strategy and related policy and procedures of the SECURE Technology Act.

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; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Maturity Level: Consistently Implemented (Level 3). The organization has consistently implemented its security architecture across the enterprise, business process, and system levels. System security engineering principles are followed and include assessing the impacts to the organizations information security architecture prior to introducing information system changes into the organization's environment.

10 of 11 [redacted] have implemented a security architecture at the bureau and information system levels. However, [redacted] did not adequately document its applicable security controls in the system security plan for one information system.

DOI can improve and increase its maturity level ensuring information security architectures are integrated with its systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the organization's information systems.

7. To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M19-03)?

Maturity Level: Managed and Measurable (Level 4) - Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement risk management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. Additionally, the organization utilizes an integrated risk management governance structure for implementing and overseeing an enterprise risk management (ERM) capability that manages risks from information security, strategic planning and strategic reviews, internal control activities, and applicable mission/business areas.

DOI has defined roles and responsibilities of risk management stakeholders such as the Chief Information Officer, Associate Chief Information Officer, Chief Information Security Officer, System Owner, and Authorizing Official. Additionally, DOI maintained the Information Management Technology Leadership Team that consists of the Bureau and Office Associate Chief Information Officer, 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 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?

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, DOI has not defined qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information, as needed, to ensure that its risks posture is maintained. DOI can improve and increase its security maturity level by defining qualitative and quantitative performance measures on the effectiveness of its POA&M activities.

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 800-39; NIST SP 800-53 REV.4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

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.

10 of 11 [redacted] perform system risk assessment and the appropriate security controls are implemented according to risk. However, [redacted] did not effectively document, implement, and assess applicable security controls for one information system that is not connected to the DOI network.

DOI can improve and increase its maturity level by consistently monitoring the effectiveness of risk responses to ensure risk tolerances are 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); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

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 to stakeholders such as Bureau and Office Associate Chief Information Officers, Chief Information Security Officers and System Owners. 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. The dashboard presents qualitative and quantitative metrics that provide indicators of risk.

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 (NIST SP 800-53 REV. 4: SA-4; NIST SP 800- 152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Maturity Level: Consistently Implemented (Level 3) - The organization ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.

10 of 11 [redacted] ensures that specific contracting language and service level agreements are included in appropriate contracts. However, [redacted] Interagency Agreement template did not contain the appropriate information security and privacy requirements.

DOI can improve and increase its maturity level by maintaining 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.

DOI has implemented a solution that provides a centralized view of risk and plan of action and milestones to support the risk management framework.

DOI can improve and increase maturity level by implementing automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to DOI systems and data.

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

The maturity level for the Risk Management function was assessed at Consistently Implemented (Level 3). One of 12 risk management metrics was assessed at Level 5: Optimized. Four of 12 risk management metrics were assessed at Level 4: Managed and Measurable. Six of 12 risk management metrics were assessed at Level 3: Consistently Implemented. One of 12 risk management metrics was assessed at Level 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 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

Maturity Level: Managed and Measurable (Level 4) - Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively. This is the highest maturity level available for this metric.

DOI has resources to adequately implement the information system configuration management activities and stakeholders are held accountable.

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 REV. 4: 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, DOI has not defined, monitored, or reported qualitative and quantitative performance measures on the effectiveness of the configuration management program.

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 REV. 4: 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.

DOI has implemented policies and procedures for managing the configuration of its information system. However, 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 REV. 4: CM-2 and CM-8; FY 2019CIO FISMA Metrics: 1.1, 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7and PR.IP-1)?

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.

10 of 11 [redacted] have implemented configuration management change control in accordance with Department Security Control Standards. However, [redacted] did not fully document and implement processes for maintaining baseline configurations and component inventory for one information system. Also, DOI is in the process of implementing an automated solution for application whitelisting. Additionally, DOI is in the process of fully implementing the policy of blocking unauthorized hardware on the network.

18. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; FY 2019CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

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 SCAP validated software assessing scanning capabilities against all systems on the network to assess and manage both code-based and configuration-based vulnerabilities.

10 of 11 [redacted] have implemented configuration management change control in accordance with Department Security Control Standards. However, [redacted] did not fully document and implement processes performing vulnerability scanning and configuration compliance checks in accordance with DOI IT security policy for one information system.

DOI can improve its maturity level by fully implementing technology that maintains a complete and accurate view of the 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 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,Control 4.5; FY 2019CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive (BOD)15-01; DHS BOD 18-02)?

Maturity Level: Consistently Implemented (Level 3) - The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities [redacted]

DOI is managing its flaw remediation process and utilizes patch management and software update tools for operating systems and third-party applications. Three of 11 [redacted] did not consistently remediate critical or high-risk vulnerabilities within [redacted] did not provide a population of security patches from which to evaluate; however, [redacted] is managing the deficiency through the Plan of Action and Milestone (POA&M) process.

DOI can improve and increase its maturity level by centrally managing its flaw remediation process and utilize automated patch management and software update tools for operating systems, where such tools are available and safe.

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 REV. 4: CM-2 and CM-3; CSF: PR.IP-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 change implementation.

10 of 11 [redacted] have implemented change control policies and procedures. One of 11 Bureaus and Offices, [redacted] did not consistently document, test, and approve system changes prior to implementation into production environment.

DOI can improve and increase its maturity level by defining 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. One of eight configuration management metrics were assessed at Level 4: Managed and Measurable. Seven of eight configuration management metrics were assessed at Consistently Implemented. The configuration management program is not effective.

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 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Maturity Level: Managed and Measurable (Level 4) - Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

DOI has defined its identity, credential, and access management roles and responsibilities through Departmental policies and manuals. Also, the DOI Access Executive Steering Committee provides oversight for 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 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

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 nonorganizational users. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.

Six of 11 [redacted] have implemented automated tools and technology to manage identity and access management. Five of 11 [redacted], [redacted] did not consistently implement procedures for account management, least privilege, or implement automated mechanisms to manage the effective implementation of its policies and procedures.

DOI can improve and increase its maturity level by ensuring all Bureaus and Offices use automated mechanisms to manage the effective implementation of its 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 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?

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

Nine of 11 [redacted] ensured personnel are assigned risk designations and appropriately screened prior to being granted system access. However, [redacted] did not consistently implement its personnel security screening procedures and [redacted] did not fully implement its personnel security program policies and procedures. [redacted] is working to remediate the weakness that was identified in the [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 REV. 4: AC-8, PL-4, and PS6)?

Maturity Level: Managed and Measurable (Level 4) - The organization uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.

Nine of 11 [redacted] use automated tools and processes with a manual component to manage and review user access agreements for privileged and non-privileged users. [redacted] did not consistently ensure user access request documentation was approved prior to system access was granted. [redacted] did not implement account management procedures for one information system.

28. To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

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

10 of 11 [redacted] utilize strong authentication for authenticating non-privileged users to applicable information systems. [redacted] did not fully implement strong authentication over non-privileged users for one information system that is not connected the DOI network.

29. To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Maturity Level: Managed and Measurable (Level 4): All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems.

10 of 11 [redacted] utilize strong authentication for authenticating privileged users to applicable information systems. [redacted] did not fully implement strong authentication over privileged users for one information system that is not connected the DOI network.

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 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

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.

Seven of 11 [redacted] have effectively implemented procedures to support the management of privileged accounts for the removal and disabling of temporary and inactive accounts. [redacted] did not consistently disable inactive user accounts for one information system. [redacted] did not effectively implement procedures for managing privileged accounts to include review of privilege user activity. The [redacted] was unable to perform a review over [redacted] personnel that have privileged access to the [redacted] computing environment to determine appropriateness. 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 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 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): Seven of nine IAM related metrics were assessed at Managed and Measurable (Level 4). Two of nine IAM metrics were assessed at Consistently Implemented (Level 3). The IAM program is effective.

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; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID. GV-3; NIST SP 800-53 REV. 4: 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 [redacted] have developed and implemented a privacy program for the protection of personally identifiable information (PII). [redacted] have not defined, documented, and implemented policies and procedures for the protection of PII. DOI can improve and increase 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 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

·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.

DOI has established a policy for protecting data in transit and data at rest; however, Bureaus and Offices have not developed implementation plans. More specifically, seven of 11 [redacted], and [redacted] had not defined and implemented procedures for the protection of its PII and other sensitive data specifically in one or more areas of encryption of data at rest, encryption of data in transit, and limitation of transfer to removable media.

DOI can improve and increase its maturity level by consistently implementing policies and procedures for the use of FIPS-validated encryption of PII and other sensitive agency data, as appropriate, both at rest and in transit, and the prevention and detection of untrusted removable media.

35. To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Maturity Level 2: Defined. The organization has defined and communicated it policies and procedures for data exfiltration, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.

DOI has implemented various technologies such as Security Incident and Event Managing software, firewalls, network monitoring tools, email and IP address filtering, and packet inspection software to monitor for unusual outbound 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 using fictional Personally Identifiable Information (PII) and determined controls to detect and prevent data exfiltration were not effective.

DOI can improve and increase its maturity level by designing and implementing controls to check outbound communications traffic to detect encrypted and non-encrypted exfiltration of information, unusual traffic patterns, and elements of PII.

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 REV. 4: 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. Also, 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 REV. 4: 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. DOI can improve and increase its maturity level by expanding the phishing exercises to include individuals responsible for PII.

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 are not effective. One of five data protection and privacy metrics was assessed at Ad Hoc (Level 1). One of five data protection and privacy metrics was assessed at Defined (Level 2). Two of five data protection and privacy metrics was assessed at Consistently Implemented (Level 3). One of five data protection and privacy metrics was assessed at Managed and Measurable (Level 4).

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 REV. 4: AT-1; and NIST SP 800-50).

Maturity Level 4: Managed and Measureable. Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

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 and stakeholders are held responsible for the program. 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 REV. 4: 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 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT- 1).

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 and maintained in the DOI Learning management system.

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 REV. 4: 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.

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 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-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 [redacted] Training records are maintained in the centralized DOI Learning management system. Also, 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 REV. 4: AT-3 and AT-4; FY 2019 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 [redacted] Training records are maintained in the centralized DOI Learning management system. Also, DOI measures the effectiveness of its security awareness training program by periodically performing phishing exercises.

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). One of eight metrics was assessed at Managed and Measurable (Level 4).

Identity and Access Management, seven of nine metrics were assessed at Managed and Measurable (Level 4). Two of nine metrics were assessed at Consistently Implemented (Level 3).

Data Protection and Privacy, one of five metrics were assessed at Managed and Measurable (Level 4). Two of five metrics were assessed at Consistently Implemented (Level 3). One of five metrics were assessed at Defined (Level 2). One of five metrics were assessed at Ad Hoc (Level 1).

Security Training, six of six metrics were assessed at Managed and Measurable (Level 4).

45. 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. Six of six security training metrics were assessed at Managed and Measurable (Level 4).
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 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?

Maturity Level: Managed and Measurable (Level 4) - The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

DOI has established an information security continuous monitoring (ISCM) strategy. Seven of 11 [redacted], [redacted] monitor and analyze performance measures over their respective ISCM programs. Four of 11 [redacted] do not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM strategy.

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 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?

Maturity Level: Managed and Measurable (Level 4) - The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and procedures and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

DOI has established an information security continuous monitoring (ISCM) strategy. Seven of 11 [redacted], [redacted] monitor and analyze performance measures over their respective ISCM programs. [redacted] have not established policies and procedures to monitor and analyze qualitative and quantitative performance measures on the effectiveness of the [redacted] ISCM program.

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 REV. 4: CA-1; NIST SP 800-137; CSF: DE. DP-1; and FY 2019 CIO FISMA Metrics)?

Maturity Level: Managed and Measurable (Level 4) - Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

DOI has implemented an ISCM program and defined roles and responsibilities and dependencies are defined, and stakeholders are accountable for carry out their responsibilities.

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 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)

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.

10 of 11 [redacted] perform organizational assessments and considers IT security controls test results as part of the ongoing authorization process. Also, results of annual security control assessments and plan of action and milestones are considered for maintaining ongoing authorization of information systems. One of 11 [redacted] has not consistently implemented its ISCM policies and procedures over one information system that is not connected to the DOI network.

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 [redacted] have not formally defined qualitative and quantitative performance metrics to measure effectiveness of the ISCM policies and procedures. Four of 11 [redacted] integrates ISCM performance metrics to deliver situational awareness across the organization.

DOI can improve and increase its maturity level by integrating metrics on the effectiveness of its ISCM program to deliver situational awareness across the organization.

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

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

51. 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 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 REV. 4: 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: 4.2; CSF: RS.RP-1; 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 and determined that the DOI Advanced Security Operation Center (ASOC) did not detect the activity. Also, the Bureaus and Offices have not fully defined qualitative and quantitative performance metrics to measure effectiveness across the organization.

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 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Maturity Level: Managed and Measurable (Level 4) – Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

DOI has implemented an incident response program. The DOI Enterprise Computer Security Incident Response Plan program defines the policies and procedures and stakeholders are accountable for managing the program. This is the highest available metric available.

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; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; 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 has not consistently implemented processes to detect and respond to suspicious network activity. Specifically, KPMG performed a data exfiltration exercise and other tests at two of 11 [redacted] and determined that [redacted] or the [redacted] did not detect the unusual and suspicious network activity.

55. How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 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 [redacted] to determine whether the DOI [redacted] would detect or block the activity. KPMG was successful in performing the tests at [redacted] without being detected. DOI can improve and increase its maturity level by consistently implementing its incident response procedures.

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 REV. 4: IR-6; US-CERT Incident Notification Guidelines;PPD-41; CSF: RS.CO-2 through 4; 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 DOI Computer Incident Response Center (DOICIRC) 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 (NIST SP 800- 86; NIST SP 800-53 REV. 4: 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 EINSTEIN 3a capabilities. This is the highest available maturity level for this metric.

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. DOI can improve and increase its maturity level by implementing technologies for monitoring and analyzing qualitative and quantitative performance metrics across the organization and report results on the effectiveness of the incident response program.

Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Consistently Implemented (Level 3). Three of seven incident response metrics were assessed at Defined (Level 2). One of seven incident response metrics were assessed at Consistently Implemented (Level 3). Three of seven incident response metrics were assessed Managed and Measurable (Level 4).

59. 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 beyond the above metrics. The incident response program is not effective.

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 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Maturity Level: Managed and Measurable (Level 4) - Resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

DOI has established a contingency plan program that require 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 accountable for their specific roles and responsibilities in contributing to the recovery of the information system and trained to respond to a contingency event. This is the highest maturity level available.

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; CSF: ID.BE-5, PR.IP-9, and ID.SC-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.

Eight of 11 [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. However, three of 11 [redacted] did not perform a functional contingency plan test in accordance with DOI IT Security Control Standards. The [redacted] information system contingency plan was not fully implemented; however, [redacted] is managing the deficiency through the Plan of Action and Milestone (POA&M) process.

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

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 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

Maturity Level: Consistently Implemented (Level 3) - The organization incorporates the results of organizational and system level [redacted] into strategy and plan development efforts consistently. System level [redacted] are integrated with the organizational level [redacted] 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 [redacted] 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 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

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 has not defined performance metrics to measure the effectiveness of the contingency plans with information on the effectiveness of related plans such as Bureau or Office continuity of operations plan or disaster recovery plan to deliver situational awareness. [redacted] does not have a contingency plan to reflect current operations for the [redacted] however, [redacted] is managing the deficiency through the Plan of Action and Milestone (POA&M) process.

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 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

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.

Eight of 11 [redacted] have implemented contingency plan testing and exercises. [redacted] conducted a contingency plan exercise in fiscal year 2019; however, the exercise did not include a functional test in accordance with the DOI Security Control Standards. The [redacted] did not fully implement its information system contingency plan; therefore, did not perform a test or exercise. DOI can improve and increase its maturity level by implementing automated mechanisms to thoroughly and effectively test system contingency plans.

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 REV. 4: 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 2019 CIO FISMA Metrics: 5.1.1; 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 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 strategies as appropriate. 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 REV. 4: CP-2 and IR-4)?

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

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.

DOI can improve and increase its maturity level by maintaining 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.

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. 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