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 2020

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

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

MAR 30 2021

Memorandum

To: William E. Vajda
Chief Information Officer

From: Mark Lee 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 2020*
Report No. 2020-ITA-032

This memorandum transmits KPMG LLP's Federal Information Security Modernization Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2020. FISMA (Pub. L. 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, at the OIG's discretion, by an independent external auditor to determine the effectiveness of such programs and practices.

KPMG, an independent public accounting firm, performed the DOI's FY 2020 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 or on KPMG's conclusions regarding DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-20-04, *Fiscal Year 2019–2020 Guidance on Federal Information Security and Privacy Management Requirements,* dated November 19, 2019.

KPMG reviewed information security practices, policies, and procedures at the DOI's 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
- Met regularly 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, the data protection and privacy program, the security training program, and contingency planning. KPMG made 32 recommendations related to these control weaknesses intended to strengthen the DOI's information security program as well as those of the bureaus and offices. In its response to the draft report, your office concurred with all recommendations and established a target completion date for each corrective action.

We will refer the recommendations to the Office of Financial Management the Office of Policy, Management and Budget to track their implementation and report to us on their status. In addition, we will notify Congress about the findings and report semiannually, as required by law, on actions you have taken to implement the recommendations and on recommendations that have not been implemented. We will also post a public version of the report on our website.

We appreciate the cooperation and assistance of DOI personnel during the audit. If you have any questions about 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 2020 Performance Audit

January 26, 2021

KPMG LLP
8350 Broad Street
McLean, Virginia 22102

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

January 26, 2021

Mr. Mark Lee Greenblatt
Inspector General
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) 2020 *Federal Information Security Modernization Act of 2014 (FISMA)* Audit for unclassified information systems**.** We performed our work during the period of April 21 to September 30, 2020 and our results are as of November 17, 2020.

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, 2020 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) FY20 Inspector General (IG) 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 select security controls identified in NIST SP 800-53 and additional security program areas identified in the 2020 IG FISMA Reporting Metrics for the OIG. We selected a sample of in-scope 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, Rev 4. DOI has an information system continuous monitoring program and incident response program. We identified needed improvements in areas audited including Risk Management (RM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), 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[1]): Identify, Protect, Detect, Respond, and Recover.[2]

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.

[1] The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

[2] In its Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST created Functions to organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

The following table summarizes the control areas tested and the control deficiencies identified in the fiscal year 2020 FISMA Reporting Metrics for the OIG.

Cybersecurity Framework Security Functions and FISMA Domain	Summary of Results
1. Identify (Risk Management)	DOI has established a risk management program. However, DOI has not fully: • Reviewed and updated policies and procedures related to the management of information system hardware inventory at [redacted] • Reviewed and updated open Plan of Action and Milestones (POA&Ms) in accordance with DOI POA&M Security Control Standards at [redacted] • Ensured the use of DOI Purchase Cards was appropriate at [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 fully: • Implemented processes and procedures to ensure system patches and updates are tested and approved prior to being deployed at [redacted]. • Updated configuration management and change management procedures at [redacted] • Implemented an effective patch and vulnerability management process to remediate vulnerabilities identified in vulnerability assessment scans at [redacted]. • Monitored, updated, and documented system baseline security requirements at [redacted] • Established an alternate processing site for one system at [redacted] • Reviewed system audit logs for suspicious or unusual activity over privileged and non-privileged users in accordance with policy at [redacted]. • Ensured relevant audit-related documentation is available for review in order to determine whether users were assigned the proper risk designation, completed the appropriate screening process, and completed the required access agreements prior to obtaining access at [redacted] • Maintained evidence of audit log reviews and evidence of follow-up actions, as appropriate at [redacted] • Ensured system-generated and manually created audit logs are reconciled for completeness and accuracy at [redacted] • Documented and implemented processes to periodically review privileged user access for appropriateness at [redacted]. • Ensured proper background investigation and screening is performed at [redacted]. • Documented and implemented procedures to support the review of privileged user activity audit logs to identify and address inappropriate or unusual activity at [redacted]. • Ensure new users obtain authorization prior to gaining system access at [redacted] • Documented and implemented procedures authorizing and provisioning new non-privileged user accounts at [redacted] • Ensured information system privacy impact assessments are reviewed and updated at [redacted] • Ensured role-based security training is completed for [redacted] privileged users at the [redacted].

3. Recover (Contingency planning)	DOI has established a contingency planning program. However, DOI has not fully: • Documented and maintained lessons learned for contingency plan tests or exercises conducted at [redacted] • Established an alternate processing site for one system at [redacted]

We have made 32 recommendations related to these control weaknesses. Our recommendations are 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 FY2019 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 FY 2020 IG FISMA Reporting Metrics.

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 several Bureaus and several additional Offices that fall under the Office of the Secretary, the Assistant Secretary for Policy, Management and Budget, Solicitor's Office and Office of Inspector General. Of those, the following 11[3] Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2020:

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.

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

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

10 The **Office of the Special Trustee for American Indians (OST)** improves the accountability and management of Indian funds held in trust by the federal government. On August 28, 2020 the office changed its name to the Bureau of Trust Fund Administration (BTFA).

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 Deputy CIO reports to the CIO and serves as the OCIO's primary liaison to Bureau Associate CIOs for day-to-day interactions between bureau leadership and OCIO's major functions.

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

Bureaus and Offices have an Associate Chief Information Officer (ACIO) that reports to the 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 OIG, 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 2020 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, 2020:

- 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, Rev. 4 controls considered during the performance audit.
- Prepare responses for each of the OMB/DHS FY 2020 IG 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 FY2020 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, Rev. 4. During this process, we assessed the implementation of a selection of security controls from the NIST SP 800-53, Rev. 4 for our representative subset (10 %) of DOI's information systems[4]. The controls selected addressed areas covered by the DHS FY2020 IG FISMA Reporting Metrics.

[4] The OIG judgmentally selected 11 of 147 operational systems of the total DOI information systems recorded in its official repository, the Cyber Security Assessment and Management tool (CSAM). 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.

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 three Cybersecurity Function areas: Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training), and Recover (Contingency Planning).

The details of the weaknesses we identified are as follows.

1. Identify Function: Implementation of the Risk Management Program.

The table below lists findings in the risk management FISMA domain.

FISMA domain	Summary of Findings
Risk Management	DOI has not consistently: • Reviewed and updated policies and procedures related to the management of information system hardware inventory at [redacted] • Reviewed and updated open Plan of Action and Milestones (POA&Ms) in accordance with DOI POA&M Security Control Standards at [redacted]. • Ensured the use of DOI Purchase Cards was appropriate at [redacted]

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

[redacted]

KPMG inspected the [redacted] procedures for maintaining information system hardware inventory to determine if a review of the procedures had been performed within the last two years of the last review date. KPMG inspected the [redacted] dated September 6, 2017, updated June 25, 2018, with an expiration date of June 25, 2020. KPMG determined that the procedure document had not been reviewed or updated within the required two-year period as required by DOI Security Control Standards.

[redacted]

KPMG selected a sample of 15 Plan of Action and Milestones (POA&Ms) from a population of 354 open POA&Ms in the Cyber Security Assessment and Management (CSAM) tool to determine whether POA&Ms were appropriately reviewed and updated. KPMG determined that 2 of 15 selected POA&Ms had not been updated quarterly with new milestones or delay justifications since December 31, 2018.

[redacted]

KPMG inspected the [redacted], which is maintained in CSAM tool. KPMG noted that one new cloud-based information system, [redacted] was procured on June 9, 2020. KPMG requested the supporting contract in an effort to ensure the service was approved in accordance with DOI policy.

KPMG inquired of management and was informed by [redacted] management that the [redacted] cloud service was purchased on a DOI "purchase credit card." Additionally, the [redacted] cloud service was not included in the [redacted] contract award inventory. KPMG inspected the DOI Purchase Card Program Policy and noted that using the government purchase cards to purchase cloud-hosting or computing services is prohibited. Therefore, the use of a purchase card to purchase the [redacted] cloud service is not compliant with DOI policy.

[redacted]

KPMG randomly selected a sample of 15 open POA&Ms from a population of 122 open POA&Ms in the CSAM tool to determine whether POA&Ms were appropriately reviewed and updated. KPMG determined that 4 of 15 selected POA&Ms, all related to the [redacted] had not been updated quarterly with new milestones or delay justifications since September 30, 2018. While the POA&Ms were reviewed September 18, 2019, KPMG determined remediation and progress to closure were not appropriately documented on a quarterly basis.

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

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

DOI Security Control Standard Configuration Management, Version 4.1, CM-8 Information System Component Inventory states:
Control: The organization:

1. Develops and documents an inventory of information system components that:
    i. Accurately reflects the current information system;
    ii. Includes all components within the authorization boundary of the information system;
    iii. Is at the level of granularity deemed necessary for tracking and reporting; and
    iv. Includes manufacturer, model number, serial number, software license information, system/component owner; and
2. Reviews and updates the information system component inventory *System Owner-defined frequency*.

DOI Security Control Standard, Security Assessment and Authorization, version 4.1, CA-5 Plan of Action and Milestones states: Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones at least quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

U.S. Department of the Interior Purchase Card Program Policy, V. Use Restrictions, A. General Restrictions, 10. Cloud hosting or computing services:

> The following restrictions apply to the use of the purchase card. Cardholders may not use the purchase card or convenience checks to complete the actions described below:
> 10. Cloud-hosting or computing services.

[redacted] management did not prioritize the review and update of the [redacted] to be performed at least every two years or by the defined expiration date in the document.

[redacted] management failed to ensure that the requirements outlined in the [redacted] POA&M Maintenance Cybersecurity Standard were implemented.

[redacted] The [redacted] contracting officer that was responsible for purchasing the [redacted] cloud service thought it was permissible in support of mission enablement due to the COVID-19 Pandemic. The contracting officer was unaware that the purchase was prohibited as stated in the DOI Purchase Card Program Policy.

[redacted] did not consistently enforce the policy requiring POA&Ms to be reviewed and updated quarterly.

[redacted] Without adequately reviewing and updating policy and procedures within the organization's defined timeframe, there is a risk that current procedures will become outdated or new requirements or processes will not be documented, to ensure the organization is adequately performing required risk mitigation activities across systems.

[redacted] Not reviewing and updating POA&Ms periodically could lead to delays in remediating and resolving known risks and vulnerabilities within the information system accreditation boundary, which could result in exploited vulnerabilities or un-remediated control deficiencies.

[redacted] Inappropriately purchasing cloud services using a government DOI purchase card circumvents the Departments cloud service contracting policy, which could lead to a lapse in security and control weaknesses.

We recommend [redacted]

1. Implement a process to ensure that Bureau hardware inventory policy and procedures are updated within the defined requirement according to the DOI Security Control Standards.

We recommend [redacted]:

2. Implement a process to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

We recommend [redacted]

3. Ensure that all contracting officers are aware of the DOI Purchase Card Policy cloud restrictions.

2. Protect Function: 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: • Implemented processes and procedures to ensure system patches and updates are tested and approved prior to being deployed at [redacted]. • Updated configuration management and change management procedures at [redacted] and [redacted] • Implemented an effective patch and vulnerability management process to remediate vulnerabilities identified in vulnerability assessment scans at [redacted]. • Monitored, updated, and documented system baseline security requirements at [redacted]

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

[redacted]

KPMG inquired of management regarding the [redacted] to determine if system security patches are evaluated in a test environment and approved prior to implementation. KPMG was informed that when new vendor system patches become available, they are simultaneously installed on the server where both development and production environments reside for the [redacted] system. KPMG determined that vendor patches are not evaluated in a test environment prior to implementation.

Also, KPMG was informed that the [redacted] was not comprehensive and did not contain procedures to facilitate the system change processes. Upon further review of the Handbook, we noted the Handbook lacked defined procedures for system changes, such as required approvals and documentation required for testing changes in a test environment prior to implementation.

KPMG obtained and reviewed five months (January 2020 – May 2020) of [redacted] vulnerability security scan results to determine whether all critical and high-risk vulnerabilities were remediated within 15 and 30 days, respectively, in accordance with [redacted] policy. KPMG judgmentally selected two months (January 2020 and February 2020) and inspected vulnerability assessment scan results for March 2020 and April 2020 to determine whether the vulnerabilities identified in January and February were remediated in the March 2020 and April 2020.

KPMG identified 101 critical and 133 high vulnerabilities during the January and February scans and determined that the same vulnerabilities were present on the April 2020 scan results, which indicates they were not remediated.

KPMG inquired of management to determine whether a process is in place to monitor and update the [redacted] baseline configuration. KPMG noted that the Center for Internet Security (CIS) Benchmark is used to establish the baseline configuration for [redacted] KPMG was informed that a script is manually run to enforce compliance to the established baseline on an ad-hoc basis. KPMG was informed that [redacted] is unable to provide evidence that the script was run at a minimum, on an annual basis, to monitor and update the baseline. KPMG determined that [redacted] does not consistently follow the process to monitor and update the baselines to the established configuration in a timely manner.

[redacted]

KPMG inspected five months (January 2020 – May 2020) of [redacted] vulnerability scans to determine whether all critical and high-risk vulnerabilities were remediated within 30 days from the patch release date or vulnerability scan date (whichever is earliest) in accordance with [redacted] policy.

KPMG judgmentally selected two months (February 2020 and March 2020) and inspected vulnerability scan results for April 2020 and May 2020 to determine whether the vulnerabilities identified in February 2020 and March 2020 were remediated in the April 2020 and May 2020 scans, evidencing remediation efforts were completed. KPMG found that 2 of 11 critical, and 4 of 42 high-risk vulnerabilities identified during the February 2020 and March 2020 scans were not remediated in April 2020 and May 2020, respectively.

[redacted]

KPMG inspected the [redacted] patch management process to determine if security patches and system updates were approved and tested prior to being implemented into the production environment. KPMG noted that patches applied to the [redacted] servers are applied to both the development and production environments simultaneously, preventing management from testing patches and updates prior to implementation.

Also, KPMG noted that 1 of 5 patches tested were not documented within the [redacted] task workflow.

KPMG noted that the [redacted] was last reviewed and updated in June 2014. KPMG determined that this was not in compliance with the DOI Security Control Standard requirement stating that configuration management policies and procedures are to be reviewed and updated at least every two years. Additionally, KPMG noted that the [redacted] does not include the [redacted] process used to document, test, approve, and implement changes to the [redacted] system.

[redacted]

KPMG inspected the population of 24 security patches for the [redacted] information system, 12 server patches and 12 operating system patches. KPMG judgmentally selected a sample of two server security patches and one operating system security patch for testing. KPMG noted [redacted] management was unable to provide evidence that the sampled security patches were tested and approved prior to deployment in the production environment.

Also, KPMG inquired of [redacted] management and was informed that application changes are not formally tested and documented.

In response to KPMG's testing, [redacted] management began developing a [redacted] site to track and document testing and approval of [redacted] patches and changes. Since the implementation of the [redacted] tracking system, no new [redacted] security patches or system changes were applied to the system. Therefore, KPMG could not perform testing to determine the effectiveness over the new change management process.

DOI Security Control Standard System Information Integrity, Version 4.1 Control SI-2 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.

CM-9 CONFIGURATION MANAGEMENT PLAN

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

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

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

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

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

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

Control: The Organization:

a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;
d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for System Owner-defined time period;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through System Owner-defined configuration change control element (e.g., committee, board) that convenes (one or more) of System Owner-defined frequency; System Owner-defined configuration change conditions.

Control Enhancements:

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

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

[redacted]

Remediation Time Frames:

To ensure effective and timely remediation of critical and high vulnerabilities identified through [redacted] scans and web reports, our mitigation timeline is:

- All Critical Vulnerabilities must be remediated within 15 calendar days of initial discovery.
- All High Vulnerabilities must be remediated within 30 days calendar of initial discovery.

DOI Security Control Standard Configuration Management Control, Version 4.1, CM-2(1) Baseline Configuration

Control Enhancements

(1) Baseline Configuration | Reviews and Updates
The organization reviews and updates the baseline configuration of the information system:

(a) At least annually;
(b) When required due to a significant change; and
(c) As an integral part of information system component installations and upgrades.

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

Control: The organization:

a. Establishes and documents configuration settings for information technology products employed within the information system using United States Government Configuration Baseline, or other appropriate checklists from the National Vulnerability Database maintained by the National Institute of Standards and Technology, that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls change to the configuration settings in accordance with organizational policies and procedures.

[redacted]

Remediation Time Frames:

Vulnerabilities must be remediated in accordance with requirements outlined in DOI Security Control Standard RA-05 and as follows:

- Zero Day – Immediately.
- Critical vulnerabilities on DMZ/Public-facing Systems – Immediately; not to exceed 15 days from vulnerability announcement.
- Critical/High – Within 30 days from patch release date or vulnerability scan date (whichever is earliest).
- Medium/Moderate – Within 90 days from patch release date or vulnerability scan date (whichever is earliest).

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.

[redacted]

17. Test, validate and document changes to systems before implementation as specified in [redacted] Configuration Management Procedures and [redacted] Software Testing Installation, Approval, and Maintenance Procedure.

DOI Security Control Standards Configuration Management, Version 4.1, CM-01 Configuration Management Policy and Procedures

Applicability: All Information 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; and
b. Reviews and updates as needed the current:
    1. Configuration management policy, at least every two years; and
    2. Configuration management procedures, at least every two years.

[redacted] Configuration Change Control Test/Validate/Document Changes

[redacted] Enterprise Services Change Advisory Boards (CAB) test, validate and document changes to Enterprise Services such as [redacted] and configurations to Enterprise software and security settings on client systems. System/SubSystem should scope procedures for this control to changes that only affect information systems within their System/SubSystem boundary.

All Systems should have a local Configuration Control Board (CCB) to manage changes within their boundary, where the CCB has processes for testing, validating and documenting changes. The [redacted] Information Security Office and Enterprise Services maintain a Fast Ring Testing process to ensure that changes are tested on a diverse sample of Windows and Mac OS X systems. Members of the Fast Ring Testing process consist of systems from centers across the country.

Changes are scheduled and applied to Fast Ring Testing systems, feedback is gathered through a Remedy feedback form process, and results are evaluated before changes are made within the environment. The Fast Ring Testing process is in place to manage risk and impact of changes before implementation to avoid costly errors from uncontrollable changes while maintain maximum uptime of infrastructure.

[redacted] has not defined and implemented a documented process to test and approve patches prior to implementation on the [redacted] servers.

Management has not designed and documented procedures to outline the process and documentation requirements for [redacted] changes such as required approvals and testing documentation.

[redacted] management indicated that, due to resources shared by various information systems that reside on a shared server and conflicting requirements and system design limitations, critical and high vulnerabilities were not remediated in a timely manner.

Based on input from [redacted] management, the baseline configuration for [redacted] is not monitored through the [redacted].[5] Therefore, a manual script is executed on an ad-hoc basis to apply and update the baseline configuration. [redacted] failed to execute the manual script annually against [redacted] as required by the policy.

[redacted] management did not prioritize remediation of critical and high-risk vulnerabilities in accordance with established [redacted] timeframes. In addition, the Service Level Agreement (SLA) related to server and workstation system-level vulnerabilities was not updated and communicated with [redacted] to ensure that system level vulnerabilities are timely remediated.

[redacted] management did not adequately document the system limitation and its inability to test [redacted] server security patches and system updates in a test environment prior to deployment into production.

KPMG inquired and was informed that the [redacted] was not reviewed and updated at least every two years, as required by DOI Security Control Standard, due to management's oversight.

[redacted] management has not opened a POA&M or drafted a formal risk acceptance to address the lack of documentation to support the information system's change and patch management policies and procedures.

[redacted] Patches not adequately tested and analyzed prior to implementation could result in a critical error, system compromises, and disruption of services.

Without a defined process, important steps to a change management process, such as testing or approval, may not occur. This could lead to potentially harmful changes that effect the operations of the system or negatively impact important mission or business functions supported by the system.

Lack of timely remediation of critical and high vulnerabilities increases the risk of system breaches that can potentially lead to exposure and/or loss of data, lack of system availability and other malicious and unauthorized activities.

Without a procedure to monitor compliance to the established baseline, [redacted] is at a risk for not being compliant with the bureau baseline configuration requirements. This increases the risk of the system becoming vulnerable to malicious attacks and/or failure.

[redacted] Without remediating critical and high-risk vulnerabilities on a timely basis, [redacted] cannot ensure the security and compliance of the system's security posture. Lack of timely remediation could put [redacted] network and assets at risk.

[redacted] Critical errors, system compromises, and disruption of services could occur if system changes are not tested and approved and the change process is not followed, documented and retained as required.

The lack of current policies and procedures may lead to inaccurate references within the respective document, resulting in relevant stakeholders referencing policy and procedure that is no longer accurate.

[redacted] Critical errors, system compromises, and disruption of services could occur if system changes are not tested and approved and the change process is not followed, documented and retained as required.

[5] [redacted] tool that is deployed across DOI.

We recommend [redacted]

4. Design and implement processes and procedures to ensure system patches and updates are tested and approved prior to being deployed to the [redacted] production environment.

5. Enhance the Configuration Management Handbook and develop change management procedures for the [redacted] system that defines requirements for documenting system change requests, obtains required approvals, and requires testing be performed.

6. Implement a process to better ensure that all critical and high-risk vulnerabilities on the [redacted] system are remediated in accordance with the timeframes established in applicable DOI Security Control Standards and [redacted] policies.

7. Monitor, update, and document [redacted] baseline requirements in accordance with DOI organizational policies and procedures.

We recommend [redacted]

8. Update the [redacted] Service Level Agreement with [redacted] to better ensure system-level vulnerabilities are remediated within the timeframes outlined in DOI Risk Assessment Security Control Standard, RA-5.

We recommend [redacted]

9. Develop a method to separate the [redacted] development and production environments to allow for appropriate testing or obtain a formal risk acceptance to address the lack of patch testing caused by [redacted] server system limitations.

10. Ensure that all [redacted] patch change requests are documented within the [redacted] ticketing system in accordance with [redacted] policy.

11. Design and implement procedures to better ensure that configuration management policy and procedure documents are reviewed, updated, and evidence of review maintained in accordance with the DOI Security Control Standard.

We recommend [redacted]

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

3. Protect Function: 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: • Reviewed system audit logs for suspicious or unusual activity over privileged and non-privileged users in accordance with policy at [redacted] • Ensured relevant audit-related documentation is available for review in order to determine whether users were assigned the proper risk designation, completed the appropriate screening process, and completed the required access agreements prior to obtaining access at [redacted] • Maintained evidence of audit log reviews and evidence of follow-up actions, as appropriate at [redacted] • Ensured system-generated and manually created audit logs are reconciled for completeness and accuracy at [redacted] • Documented and implemented processes to periodically review privileged user access for appropriateness at [redacted]. • Ensured proper background investigation and screening is performed at [redacted] • Documented and implemented procedures to support the review of privileged user activity audit logs to identify and address inappropriate or unusual activity at [redacted]. • Ensured new users obtain authorization prior to gaining system access at [redacted] • Documented and implemented procedures authorizing and provisioning new non-privileged user accounts at [redacted]

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

[redacted]

KPMG inquired of management whether reviews of system-generated audit logs for the [redacted] system are performed [redacted] to assist in timely identification and resolution of unauthorized or unusual privileged user activity. KPMG was informed that audit logs were reviewed on an ad-hoc basis and that reviews were not documented and maintained.

KPMG obtained and reviewed the [redacted] user listing and determined the listing lacked key information required to perform testing. The listing did not include a user account status (enabled vs disabled) or account creation date, and KPMG was unable to differentiate between non-privileged and privileged users. After several attempts to provide a complete and accurate user listing, [redacted] management was unable to satisfy the request. Without the complete [redacted] user listing, KPMG was unable to perform test procedures to determine whether users were assigned the proper risk designation, completed the appropriate screening process, and completed the required access agreements prior to obtaining access to [redacted]

[redacted]

KPMG inquired of management regarding the [redacted] system to determine whether reviews of system generated user audit logs are performed [redacted] to assist in timely identification and resolution of unauthorized or unusual system activity. KPMG was informed that system generated user activity audit logs and a manual log of shared service account activity were reviewed on a monthly basis.

KPMG noted the following audit and accountability control deficiencies:

- The frequency of audit log reviews is not performed [redacted] in accordance with policy;
- Evidence of audit log reviews are not maintained; and
- Management does not have a process in place for [redacted] to perform a reconciliation between the manual review of shared system account activity and the [redacted] automated audit log to ensure that documented information is complete and accurate.

KPMG inspected the user listing for [redacted] and noted there were a total of 13 privileged users. KPMG inquired of management and was informed that 9 of 13 privileged users, such as the [redacted] and [redacted] access, was inappropriate and access was not disabled or removed in a timely manner.

KPMG inquired of [redacted] management to determine if the level and the type of background investigation for privileged and non-privileged users was appropriate. KPMG randomly sampled 17 of 68 users and determined that one user did not have the appropriate investigation prior to obtaining access to [redacted] A [redacted] investigation was performed in 2010 for the user. However, the user's current position requires a [redacted] investigation, designated as a low-risk, non-sensitive. KPMG was informed that a [redacted] investigation cannot be accepted as a reciprocity for a [redacted] because the [redacted] does not capture the adequate information required for a competitive service position.

[redacted]

KPMG inquired as to whether policies and procedures have been established to support the regular monitoring and review of [redacted] privileged user activity. KPMG was informed that [redacted] management had not established procedures or processes to support the review of privileged user activity audit logs. Privileged user activity audit logs are produced on an ad-hoc basis for investigative purposes.

KPMG inspected a selection of new [redacted] user accounts to determine if access was properly provisioned. KPMG noted that 140 new [redacted] user accounts were created. KPMG tested a random sample of new users and noted that 2 of 15 new users were granted access to the [redacted] system prior to receiving formal authorization.

[redacted]

KPMG inquired as to whether policies and procedures have been established that require regular monitoring and review of [redacted] privileged account activity. KPMG was informed that [redacted] management had not established procedures or processes to support the periodic review of privileged user activity audit logs. Privileged user activity audit logs are produced on an ad-hoc basis for investigative purposes. Management indicated no formal procedures have been established.

KPMG inspected evidence of the risk designation assigned to the [redacted] system users to determine if the appropriate level of background check was performed. KPMG obtained a population of 54 new [redacted] users who were provisioned access to the [redacted] system during the period of October 1, 2019,

through September 30, 2020. KPMG randomly selected a sample of five [redacted] new users and inspected evidence of their Position Description Records (PDRs) and background investigations. KPMG noted that 1 of 5 users received a [redacted] investigation when a [redacted] investigation was required.

[redacted]

KPMG inquired of [redacted] management and management to determine if policy and procedures have been established requiring regular monitoring and review of privileged account activity for the [redacted] KPMG was informed that [redacted] management has not established procedures or processes related to the periodic review of privileged user activity audit logs.

Also, KPMG obtained and inspected [redacted] policy documents related to audit and accountability controls and noted that the [redacted] management team has not developed procedures for reviewing privileged user activity audit logs. Privileged user activity audit logs are produced on an ad-hoc basis for investigative purposes.

[redacted]

KPMG inquired of the [redacted] to determine whether account management controls are in place over the security tools supporting the DOI [redacted] efforts; specifically [redacted] is used for asset, configuration, and patch management. [redacted] is used to monitor the DOI network for unauthorized servers, workstations, and networked devices connected to the network.

KPMG was informed that [redacted] user accounts were not reviewed for compliance and reauthorized access in accordance with DOI policy. There are 79 privileged and non-privileged [redacted] users and 22 privileged and non-privileged [redacted] users.

[redacted]

KPMG inquired of [redacted] management to determine whether there are procedures established for ensuring access agreements are completed for non-privileged user accounts. KPMG was informed that there was no formal user access authorization in place for non-privileged users. There are approximately 38 non-privileged [redacted] users. The [redacted] in charge of each [redacted] submits a request to have a new user provisioned verbally or through an email. In addition, KPMG was informed that a record of the emails is not maintained.

KPMG inquired of [redacted] to determine whether reviews of system generated user audit logs are performed at least [redacted] to assist in timely identification and resolution of unauthorized system activity. KPMG was informed that the review of the audit logs is not documented and maintained.

DOI Security Control Standards Audit and Accountability, Version 4.1, AU-6 Audit Review, Analysis, and Reporting

Applicability: All Information Systems

Control: The organization:

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

b. Reports findings to designated organizational officials.

Government Accountability Office (GAO) Government Auditing Standards Chapter 1: Foundation and Principles for the Use and Application of Government Auditing Standards 1.03:

> As reflected in applicable laws, regulations, agreements, and standards, management and officials of government programs are responsible for providing reliable, useful, and timely information for transparency and accountability of these programs and their operations. Legislators, oversight bodies, those charged with governance, and the public need to know whether (1) management and officials manage government resources and use their authority properly and in compliance with laws and regulations; (2) government programs are achieving their objectives and desired outcomes; and (3) government services are provided effectively, efficiently, economically, and ethically.

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government Documentation of the Internal Control System:

> 3.09 – Management develops and maintains documentation of its internal control system.
>
> 3.10 – Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

NIST Special Publication 800-53 Rev 4. Security and Privacy Controls for Federal Information System and Organizations, PS-3 Personnel Screening

The organization:

a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

DOI Security Control Standards Access Control, Version 4.1, AC-2 Account Management

> Applicability: All Information Systems
>
> 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 authorization (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 Access Control, 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 Standards Access Control, Version 4.1, AC-6 (5) Privileged Accounts

Control: The organization restricts privileged accounts on the information system to *System Owner-defined personnel or roles*.

Office of Personnel Management Federal Investigative Services Notice No.12-01:

Employment Suitability adjudications require character and conduct information not collected in the [redacted] investigation; therefore, when the [redacted] is the previous investigation, and the person is seeking a competitive service position which requires a [redacted] for a suitability determination, a [redacted] must be requested to provide all required information.

[redacted] Based on input from [redacted] management, [redacted] did not have adequate resources to effectively perform [redacted] audit log reviews to determine whether system anomalies and incidents were researched and/or investigated.

The [redacted] Team did not provide complete and adequate evidence within the period designated by the auditors in order to perform test procedures over the risk designation and screening process.

[redacted] Based on input from [redacted] management, [redacted] audit logs contain a large volume of information and data, making it difficult to effectively review and analyze. [redacted] management did not develop a process to perform a reconciliation between the manual audit log and the [redacted] audit log to ensure that documented information was complete and accurate.

The nine users with privileged access to the [redacted] system were initially members of the implementation team for the [redacted] system, where that level of access was appropriate. At some point, the privileged access was no longer required; however, they did not submit a request to have their access removed. Furthermore, a procedure has not been implemented that identifies when a user's access requirements change or becomes obsolete over time.

Based on input from [redacted] management, a regional suitability adjudicator did not effectively identify that a [redacted] investigation was required for the job description.

[redacted] Based on input from [redacted] management, [redacted] management did not prioritize and develop a process to perform privileged user activity audit log reviews.

KPMG was informed that, due to their oversight, [redacted] management did not enforce the established [redacted] account management policies and procedures that require new system access to be authorized prior to being provisioned.

[redacted] KPMG was informed that [redacted] management is in the process of transitioning several functions required by the Audit and Accountability control family, such as privileged user activity audit log reviews, to a central [redacted] tool and team.

In regard to the risk designation weakness identified; the sampled user's risk designation reinstatement actions were performed prior to the establishment of the current [redacted] process. As a result, the user's increased background investigation requirement was overlooked by management.

[redacted] management did not prioritize the development and implementation of audit and accountability controls to meet DOI Security Control Standards.

[redacted] The [redacted] failed to conduct the required annual account review process for [redacted] users to ensure access is valid and appropriate.

[redacted] did not effectively document and implement access authorization procedures over the [redacted] system. Also, [redacted] indicated that audit log reviews are performed; however, [redacted] was unable to provide evidence of audit log reviews.

[redacted] Without the timely identification of unauthorized and/or inappropriate user activity, there is an increased exposure to potential system failures, data loss, and corruption. The lack of explicitly documented reviews could result in the review process not being performed timely and potentially allowing inappropriate and/or unauthorized activity to be missed.

Without the completion of all testing during the annual FISMA audit, the risk of not identifying gaps in management's processes and procedures is significantly increased. Consequently, potential vulnerabilities may not be identified that could lead to system compromise, data exposure, loss of data, reputational damage, and ultimately the inability for [redacted] to fulfill their mission requirements.

Without performing risk designation and screening users, the risk of an employee not being properly vetted is increased, which could lead to the bureau experiencing insider threat related issues that can lead to unauthorized and/or inappropriate activity in the system environment.

Without ensuring that access agreements are completed and approved, there is an increased risk of unauthorized and/or inappropriate access to the [redacted] application.

[redacted] Without the timely identification of unauthorized and/or inappropriate user activity, there is an increased exposure to potential system failures, data loss and corruption. Furthermore, without the reconciliation of manual logs to system generated reports, the potential for missing and inaccurate information being misinterpreted as complete and accurate is high. This could also result in potential system failures, data loss, and corruption. The lack of explicitly documented reviews could result in the review process not being performed timely and potentially allow inappropriate and/or unauthorized activity to be missed.

The lack of a process that identifies and addresses user access that becomes inappropriate for his or her job requirements creates the risk that a user could perform unauthorized and/or inappropriate activity in the system. This could lead to the loss and/or corruption of data and potential damage to the system.

Performing an investigation that is inappropriate for the job position increases the risk that an employee is not being properly vetted, which could lead to the bureau experiencing insider threat related issues that can lead to unauthorized and/or inappropriate activity in the system environment.

[redacted] The lack of adequate procedures to ensure user activity is reviewed and analyzed increases the risk of inappropriate user activity not being detected, which could lead to unauthorized and inappropriate activity on the [redacted] system.

A user who obtains system access prior to receiving authorization are at risk of receiving system access that is not commensurate with the user's roles and responsibilities.

[redacted] The lack of adequate procedures to ensure privileged and non-privileged user activity is reviewed and analyzed on a [redacted] basis increases the risk of inappropriate user activity not being detected, which could lead to unauthorized and inappropriate activity on the [redacted] system.

Position designations, position designation records, 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 the review is 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 [redacted]

[redacted] The lack of adequate procedures to ensure privileged and non-privileged user activity is reviewed and analyzed on a [redacted] basis increases the risk of inappropriate user activity not being detected, which could lead to unauthorized use of the [redacted] system and data.

[redacted]: Failure to review and reauthorize user accounts increases the likelihood of unauthorized access, modification, and deletion of DOI data and information.

[redacted] Without a formal user access authorization procedure in place that includes the documentation of the request and approval of user access, there is an increased risk of unauthorized and/or inappropriate access to the [redacted] application.

We recommend [redacted]

13. Design and implement a process to perform [redacted] audit log reviews of all [redacted] user activity.

14. Complete a [redacted] or obtain a formal risk acceptance noting the [redacted] limitation to generate a user listing that includes account creation date, privileged and non-privilege identifier, and whether the account is enabled or disabled.

We recommend [redacted]

15. Ensure [redacted] audit log reviews are documented to include the user and date of the review, evidence of any follow-up actions required, and that users performing the review are not reviewing their own activity.

16. Develop and implement a process for the reviews of manually created audit logs and perform a reconciliation between system-generated audit logs and the manual logs to ensure all activities are completely and accurately captured.

17. Design and implement a process to periodically review all [redacted] user access to determine if the access is appropriate.

18. Design and implement a process to ensure that [redacted] user access is modified as needed when a user transfers within [redacted] or when roles and responsibilities change.

19. Implement a process to ensure the appropriate personnel screening of individuals is performed as it relates to job responsibilities, prior to authorizing system access.

We recommend [redacted]

20. Design and implement procedures to ensure [redacted] audit logs containing privileged and non-privileged user activity are reviewed and analyzed, in accordance with DOI policy, to identify and address inappropriate or unusual activity.

21. Enforce current account management policy and procedures that require new [redacted] system access to be authorized prior to being provisioned.

We recommend [redacted]

22. Design and implement audit and accountability policies and procedures to ensure [redacted] audit logs containing privileged and non-privileged user activity are reviewed and analyzed for inappropriate or unusual activity in accordance with DOI Security Control Standards.

23. Enhance the position risk designation and user screening process to ensure all [redacted] users receive the appropriate level of background investigation in accordance with their respective position risk designations and the bureau's [redacted] process.

We recommend [redacted]

24. Design and implement procedures to ensure [redacted] audit logs are reviewed and analyzed on a [redacted] basis for inappropriate or unusual privileged and non-privileged user activity and to report findings to the appropriate official.

We recommend [redacted]

25. Design and implement a process to review all [redacted] user accounts at least annually, to determine whether access is valid and appropriate.

We recommend [redacted]

26. Define, document, and implement a formal process for authorizing and provisioning non-privileged user's access to the [redacted] information system.

27. Ensure [redacted] audit log reviews are performed and documented, to include the user and date of the review, evidence that identified unauthorized activity is addressed and resolved, and that users performing the review are not reviewing their own activity.

4. Protect Function: Implementation of the Data Protection and Privacy Program.

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

FISMA Domain	Summary of Findings
Data Protection and Privacy	DOI has not consistently ensured information system privacy impact assessments are reviewed and updated at [redacted]

KPMG performed the following procedures and noted the following weaknesses in one of eleven Bureaus and Offices' data protection and privacy programs: [redacted]

[redacted]

KPMG inquired of [redacted] management to determine whether the Privacy Impact Assessment (PIA) was reviewed and updated periodically so that potential privacy risks are addressed, and appropriate privacy controls are implemented. KPMG was informed that the last PIA for [redacted] was conducted and documented in 2009, significantly exceeding the minimum required review period of 3 years.

DOI Privacy Impact Assessment Guide, Departmental Privacy Office, Office of the Chief Information Officer (OCIO), Section 1.0 – What is a Privacy Impact Assessment (PIA)

> The PIA process requires collaboration between the information System Owner, Program Manager, Information System Security Officer, the Bureau/Office Records Officer, the Bureau/Office Privacy Officer, and the departmental Privacy Office to ensure potential privacy risks are addressed and appropriate privacy protections are implemented.
>
> PIAs must be updated when changes are made to systems that may raise new privacy risks, when there is a change in information handling practices or information collection, or at a minimum at least every three years.

DOI Privacy Control Standards, version 1.0, AR-2 Privacy Impact and Risk Assessment

> Control: The organization:
> a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
> b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

[redacted] Privacy procedures were not implemented that ensured the review and update of the PIA.

[redacted] An updated PIA is necessary to identify how PII is collected, maintained, and used. Without it, there is an increased risk that PII in use may be unidentified, misused, or erroneously distributed, which can potentially result in security, privacy, and reputational risks to the bureau and department.

We recommend [redacted]

28. Ensure the privacy impact assessment for [redacted] is performed and implement a process to ensure the PIA is reviewed and updated in accordance with DOI privacy policies.

5. Protect Function: Implementation of the Security Training Program.

The table below lists findings in the security training program.

FISMA Domain	Summary of Findings
Security Training	DOI has not consistently ensured role-based security training is completed for [redacted] privileged users at the [redacted].

KPMG performed the following procedures and noted the following weaknesses in one of eleven Bureaus and Offices' security training program: [redacted]

[redacted]

KPMG inquired of the [redacted] to determine whether [redacted] privileged user access is reviewed and approved at least annually in accordance with DOI account management policies. Privileged users included domain, system, and workstation administrators.

KPMG was informed that the Role-Based Security Training (RBST) mechanism is used to evidence review of [redacted] privileged users for compliance with account management requirements. KPMG randomly selected 25 of 367 [redacted] privileged users and noted 10 of 25 sampled privileged users did not complete their RBST for the annual recertification requirement.

DOI Security Control Standard: Account Management, Version 4.1: AC-2 Account Management:

Applicability: All Information Systems

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 authorization (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

[6] [redacted] is used to manage computers and other devices on the DOI network. [redacted] allows network administrators to create and manage domains, users, devices, and objects on the network.

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.

[redacted]: The [redacted] did not complete [redacted] privilege user reviews for compliance with account management requirements at least annually.

[redacted]: Without effectively reviewing privileged user listings, roles and permissions, unauthorized individuals may have retained access after being transferred, or maintain privileges that are no longer required.

We recommend [redacted]

29. Document and implement a process to ensure that [redacted] privileged users are reviewed for compliance with account management requirements, in accordance with DOI Security Control Standards.
30. Ensure [redacted] privileged users' complete role-based security training in accordance with DOI security training policies.

6. Recover Function: Implementation of the Contingency Planning Program.

The table below lists findings in the contingency planning program.

FISMA Domain	Summary of Findings
Contingency Planning	DOI has not consistently: • Documented and maintained lessons learned for contingency plan tests or exercises conducted at [redacted] • Established an alternate processing site for one system at [redacted]

KPMG performed the following procedures and noted the following weaknesses in two of eleven Bureaus and Offices' contingency planning program: [redacted].

[redacted]

KPMG reviewed the [redacted] 2019, and noted that the plan did not include policies or procedures to support the completion of a lessons learned activity as part of the contingency plan test exercise.

KPMG also obtained and reviewed the [redacted] performed in [redacted] 2020 and noted that the exercise results did not include lessons learned documentation.

[redacted]

KPMG inquired of [redacted] management and inspected the Backup and Recovery Procedures for the [redacted] to determine whether the primary and secondary processing sites supporting the system are adequately separated so that a threat affecting one facility would not likely affect the other, ensuring the [redacted] system's availability.

KPMG noted that the primary and alternate processing sites for [redacted] are within a [redacted]-mile radius [redacted] making them subject to the same general threats, including physical, cybersecurity risks, and natural disasters

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 800-53 revision 4: CP-7

Relevant excerpts from NIST guidance:

CP-7 ALTERNATE PROCESSING SITE Control Enhancements 1-3:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE
The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.
(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY
The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE
The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

[redacted] management did not require the documentation of lessons learned be included in the [redacted], which led to the lessons learned process not being appropriately documented within the [redacted] test exercise.

[redacted] The lack of a documented lessons learned process presents a risk that contingency plan failures identified within the contingency plan test exercise are not adequately addressed and remediated. This increases the risk of the Contingency Plan not operating as expected and/or failing.

[redacted] management intentionally located the alternate processing site in [redacted], close to the primary site in [redacted] in order to utilize [redacted] staff to support the alternate site.

[redacted] planned to relocate the alternate site to a geographically separate location; however, the relocation of the alternate site was not realized, leaving both the alternate and primary sites in proximity of one another with no scheduled plan for relocation.

[redacted] Due to the close geographical proximity of the primary and alternate processing sites to one another, they are both likely subject to the same threats posed by natural disaster events. In the event of a disaster, both the primary and alternate processing sites could be compromised and cause the [redacted] system to be unavailable for an extended period.

We recommend [redacted]

31. Update the [redacted] to include procedures to document the lesson learned process in support of the [redacted] test exercise.

We recommend [redacted]

32. Identify and relocate the alternate processing sites for [redacted] to a location that is geographically separated from the primary processing site to limit susceptibility to the same threats.

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, data protection and privacy, security training, and contingency planning.

The Department of the Interior's Management Response to the Fiscal Year 2020 Draft OIG FISMA Performance Audit Report, 2020-ITA-032

Below are the recommendations (**bold**) from the report, bureau management responses (*italic*) from the report, assignment of responsible official herein, and target completion dates herein. Each responsible official assigned is the Deputy or Associate Chief Information Officer (ACIO) for the bureau or office(s) that received the recommendations.

Recommendation 1. Implement a process to ensure that Bureau hardware inventory policy and procedures are updated within the defined requirement according to the DOI Security Control Standards.

[redacted] *Management Response (1): Concur.*

Responsible Official: [redacted] *ACIO; Target Completion Date: November 30, 2021. CIO concurs with management's response and notes that the* [redacted] *document was due to be updated by* [redacted]*, 2020.*

Recommendation 2. Implement a process to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

[redacted] *Management Response (2): Concur. In* [redacted] *2020,* [redacted] *leadership delivered briefings to the* [redacted] *that stressed the importance of managing POA&Ms on a quarterly basis. In addition,* [redacted] *recently created a dashboard in* [redacted] *to identify POA&Ms that have not been reviewed and updated quarterly in accordance with DOI policy. In order to strengthen compliance, we will investigate the use of automatic alerts that can be sent to the* [redacted] *and the* [redacted] *FISMA Compliance team when a POA&M has not been reviewed in the required timeframe. We will also investigate modifying our Delayed POA&M dashboard to send automatic alerts when Planned Finish dates for POA&Ms are in the past and require an update. To ensure this issue receives an appropriate amount of attention we will also add a Quarterly POA&M review metric into the* [redacted]*. To directly address this finding, we will open a POA&M to address the two POA&Ms that had not been updated quarterly with new milestones or delay justifications since December 31, 2018.*

Responsible Official: [redacted] *ACIO; Target Completion Date: August 1, 2021. CIO concurs with management's response.*

Recommendation 2. Implement a process to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

[redacted] *Management Response: Concur (2).* [redacted] *will implement the following updates to the POA&M review process:*

- *All* [redacted] *System Owners will be briefed by the Information System Security Officer (ISSO) on a* [redacted] *basis, ensuring that all open POA&Ms and all related milestones are reviewed and updated.*

- *The ISSO will be required to submit a [redacted] statement per the established deadline, to the Information Security Office certifying that the System Owner has been briefed on the security posture of the system for the current [redacted] The briefing must include an update on the status of open POA&Ms, asserting that review/update has been performed. All dates associated with the POA&Ms, including milestones, must be updated.*
- *For systems that do not meet the updated requirements, a letter of non-compliance will be issued to the System Owner with a Cc to the [redacted] Authorizing Official.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021 CIO Concurs with management's response.

Recommendation 3. Ensure that all contracting officers are aware of the DOI Purchase Card Policy cloud restrictions.

[redacted] *Management Response (3): Concur. [redacted] will ensure all contracting officers are notified that DOI Purchase Card Policy prohibits purchasing cloud services using a government credit card.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021

CIO Concurs with management's response. Additionally, the [redacted] Deputy CIO (DCIO) for Program Management (PMD) will follow up with Senior Procurement Executive to consider additional [redacted] internal controls.

Recommendation 4. Design and implement processes and procedures to ensure system patches and updates are tested and approved prior to being deployed to the [redacted] production environment.

[redacted] *Management Response (4): Concur.*

Responsible Official: [redacted] ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.

Recommendation 5. Enhance the Configuration Management Handbook and develop change management procedures for the [redacted] system that defines requirements for documenting system change requests, obtains required approvals, and requires testing be performed.

[redacted] *Management Response (5): Concur.*

Responsible Official: [redacted] ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.

Recommendation 6. Implement a process to better ensure that all critical and high-risk vulnerabilities on the [redacted] system are remediated in accordance with the timeframes established in applicable DOI Security Control Standards and [redacted] policies.

[redacted] *Management Response (6): Concur.*

Responsible Official: [redacted] ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.

Recommendation 7. Monitor, update, and document [redacted] baseline requirements in accordance with DOI organizational policies and procedures.

[redacted] *Management Response (7): Concur.*

Responsible Official: [redacted] *ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.*

Recommendation 8. Update the [redacted] with [redacted] to better ensure system-level vulnerabilities are remediated within the timeframes outlined in DOI Risk Assessment Security Control Standard, RA-5.

[redacted] *Management Response (8): Concur.* [redacted] *Information System Security Officer will review current processes to ensure system vulnerabilities are remediated and validated in accordance within the established timeframes. To address server and workstation vulnerabilities* [redacted] *will update their* [redacted] *with* [redacted] *to ensure system level vulnerabilities are remediated within the timeframes outlined in DOI Security Control Standard RA-05.*

Responsible Official: [redacted] *ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.*

Recommendation 9. Develop a method to separate the [redacted] development and production environments to allow for appropriate testing or obtain a formal risk acceptance to address the lack of patch testing caused by [redacted] server system limitations.

Recommendation 10. Ensure that all [redacted] patch change requests are documented within the [redacted] ticketing system in accordance with [redacted] policy.

[redacted] *Management Response (9 & 10): Concur.* [redacted] *is in the process of upgrading and migrating from the* [redacted] *operating system and the* [redacted] *hardware. Several* [redacted] *servers have been purchased and will allow the existing* [redacted] *contractor to apply operating system patches in a more phased approach.*

Responsible Official: [redacted] *ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.*

Recommendation 11. Design and implement procedures to better ensure that configuration management policy and procedure documents are reviewed, updated, and evidence of review maintained in accordance with the DOI Security Control Standard.

[redacted] *Management Response (11): Concur. The* [redacted] *will be reviewed/updated accordingly and every two years thereafter.*

Responsible Official: [redacted] *ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.*

Recommendation 12. Enforce the established configuration management plan that requires [redacted] security patches and application changes to be documented, tested, and approved through the [redacted] change management process.

[redacted] *Management Response (12): Concur.* [redacted] *will move forward accordingly.*

Responsible Official: [redacted] *ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.*

Recommendation 13. Design and implement a process to perform [redacted] audit log reviews of all [redacted] user activity.

[redacted] *Management Response (13): Concur.*

Responsible Official: [redacted] *ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.*

Recommendation 14. Complete a [redacted] or obtain a formal risk acceptance noting the [redacted] limitation to generate a user listing that includes account creation date, privileged and non-privilege identifier, and whether the account is enabled or disabled.

[redacted] *Management Response (14): Concur.*

Responsible Official: [redacted] *ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.*

Recommendation 15. Ensure [redacted] audit log reviews are documented to include the user and date of the review, evidence of any follow-up actions required, and that users performing the review are not reviewing their own activity.

Recommendation 16. Develop and implement a process for the reviews of manually created audit logs and perform a reconciliation between system-generated audit logs and the manual logs to ensure all activities are completely and accurately captured.

[redacted] *Management Response (15 & 16): Concur.* [redacted] *will work with support team to develop an efficient automated audit log reporting capability that can be reviewed on a weekly basis. Documentation of review will be included. The manual log process for the* [redacted] *review will be replaced by the above referenced automated process.*

Responsible Official: [redacted] *ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.*

Recommendation 17. Design and implement a process to periodically review all [redacted] user access to determine if the access is appropriate.

Recommendation 18. Design and implement a process to ensure that [redacted] user access is modified as needed when a user transfers within [redacted] or when roles and responsibilities change.

[redacted] *Management Response (17 & 18): Concur. We will develop and implement a process for reviewing privileged access on a [redacted] basis. The [redacted] will develop and implement a process to ensure all users access is reviewed and approved on an annual basis.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 19. Implement a process to ensure the appropriate personnel screening of individuals is performed as it relates to job responsibilities, prior to authorizing system access.

[redacted] *Management Response (19). Concur. [redacted] will take the following measures:*

- *Provide training to adjudicators on the appropriate personnel screening of individuals as it relates to job responsibilities and ensuring proper investigations are performed.*
- *Initiate an immediate [redacted] investigation of the employee identified as not having the appropriate investigation.*
- *Review the remaining [redacted] users that were not included in the KPMG sample to ensure appropriate investigations have been completed as appropriate.*
- *If any additional users are identified as not having appropriate investigations commensurate with their responsibilities, investigations will be initiated in accordance with requirements.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 20. Design and implement procedures to ensure [redacted] audit logs containing privileged and non-privileged user activity are reviewed and analyzed, in accordance with DOI policy, to identify and address inappropriate or unusual activity.

[redacted] *Management Response (20): Concur. [redacted] is working toward implementing the [redacted] product for monitoring unusual activity. Additional dashboards will be created so the [redacted] contractors can easily view and monitor privileged user activity.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 21. Enforce current account management policy and procedures that require new [redacted] system access to be authorized prior to being provisioned.

[redacted] *Management Response (21): Concur. Currently there is no link between the on-boarding process and the [redacted] authorization request. We will analyze and correct the [redacted] application so that [redacted] accounts cannot be granted unless a user is fully on-board.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 22. Design and implement audit and accountability policies and procedures to ensure [redacted] audit logs containing privileged and non-privileged user activity are reviewed and analyzed for inappropriate or unusual activity in accordance with DOI Security Control Standards.

[redacted] *Management Response (22): Concur. The [redacted] plan for* corrective action includes the following:

- *The [redacted] will coordinate with [redacted] branch to transition several functions required by the AU control family, such as privileged user activity audit log reviews, to a central [redacted] tool and team.*
- *The [redacted] will document procedures to ensure privileged and non-privileged user activity is reviewed and analyzed on a [redacted] basis.*
- *The estimated planned start date is November 1, 2020 with planned implementation by June 30, 2021. [redacted] plans full compliance and closure of the [redacted] by September 30, 2021.*

Responsible Official: [redacted] ACIO; Target Completion Date: October 1, 2021. CIO Concurs with management's response.

Recommendation 23. Enhance the position risk designation and user screening process to ensure all [redacted] users receive the appropriate level of background investigation in accordance with their respective position risk designations and the bureau's [redacted] process.

[redacted] *Management Response: Concur. With the establishment of [redacted] there are processes and procedures in place as to the [redacted] flowing through the process to [redacted], so that a correct investigation is performed. HR will get the required information from the employee's Supervisor and initiate the correct [redacted] investigation. The planned start date is 10/16/2020 and the planned finish date is 06/16/2021.*

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 24. Design and implement procedures to ensure [redacted] audit logs are reviewed and analyzed on a [redacted] basis for inappropriate or unusual privileged and non-privileged user activity and to report findings to the appropriate official.

[redacted] *Management Response (24): Concur. The [redacted] team already has an initial draft of an updated process to address this finding underway. We fully expect implementation of an updated SOP and process to resolve this recommendation before September 30, 2020.*

Responsible Official: [redacted] ACIO; Target Completion Date: October 1, 2021. CIO Concurs with management's response.

Recommendation 25. Design and implement a process to review all [redacted] user accounts at least annually, to determine whether access is valid and appropriate.

[redacted] Management Response (25): Concur. The [redacted] will design and implement a process to review all [redacted] user accounts at least [redacted] to determine whether access is valid and appropriate.

Responsible Official: DOI CISO; Target Completion Date: October 1, 2021. CIO Concurs with management's response.

Recommendation 26. Define, document, and implement a formal process for authorizing and provisioning non-privileged user's access to the [redacted] information system.

Recommendation 27. Ensure [redacted] audit log reviews are performed and documented, to include the user and date of the review, evidence that identified unauthorized activity is addressed and resolved, and that users performing the review are not reviewing their own activity.

[redacted] Management Response (26 & 27): Concur. [redacted] will move forward accordingly.

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 28. Ensure the privacy impact assessment for [redacted] is performed and implement a process to ensure the PIA is reviewed and updated in accordance with DOI privacy policies.

[redacted] Management Response (28): Concur. [redacted] has completed an up to date draft PIA and requested a review meeting with DOI Privacy in accordance with DOI Privacy Program procedures.

Responsible Official: [redacted] ACIO; Target Completion Date: November 30, 2021. CIO Concurs with management's response.

Recommendation 29. Document and implement a process to ensure that [redacted] privileged users are reviewed for compliance with account management requirements, in accordance with DOI Security Control Standards.

Recommendation 30. Ensure [redacted] privileged users' complete role-based security training in accordance with DOI security training policies.

[redacted] Management Response (29 & 30): Concur.

Responsible Official: [redacted]; Target Completion Date: October 1, 2021. CIO Concurs with management's response.

Recommendation 31. Update the [redacted] to include procedures to document the lesson learned process in support of the [redacted] test exercise.

[redacted] Management Response (31): Concur.

Responsible Official: [redacted] ACIO; Target Completion Date: August 1, 2021. CIO Concurs with management's response.

Recommendation 32. Identify and relocate the alternate processing sites for [redacted] to a location that is geographically separated from the primary processing site to limit susceptibility to the same threats.

[redacted] *Management Response (32): Concur. We will begin working towards creating the necessary POA&Ms and closing these findings.*

Responsible Official: [redacted] *ACIO; Target Completion Date: October 1, 2021. CIO Concurs with management's response.*

Appendix I – Summary of Program Areas Bureaus and Offices Have Control Deficiencies

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 FY2020 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]
Identify		X	X	X							X
Protect		**X**	**X**	X	**X**	X		**X**			**X**
Detect											
Respond											
Recover				X							

Legend: X – Weakness identified in Cybersecurity function

Appendix II – Listing of Acronyms

Acronym	Definition
AC	Access Control
ACIO	Associate Chief Information Officer
ACISO	Associate Chief Information Security Officer
[redacted]	[redacted]
[redacted]	[redacted]
AICPA	American Institute of Certified Public Accounts
AU	Audit and Accountability
[redacted]	[redacted]
BIA	Bureau of Indian Affairs
BIA	Business Impact Assessment
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
CA	Security Assessment and Authorization
CAB	Change Advisory Board
CCB	Change Control Board
[redacted]	[redacted]
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CR	Change Request
CSAM	Cyber Security Assessment and Management

CVE	Common Vulnerability and Exposures
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DOI	United States Department of the Interior
DPP	Data Protection and Privacy
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
[redacted]	[redacted]
FWS	US Fish and Wildlife Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GSS	General Support System
[redacted]	[redacted]
HVA	High Value Asset
IA	Identification and Authentication
IA	Information Assurance
IAM	Identity and Access Management
IBM	International Business Machines
ID	Identifier
[redacted]	[redacted]
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
IT	Information Technology

[redacted]	[redacted]
KPMG	KPMG LLP
LAN	Local Area Network
[redacted]	[redacted]
[redacted]	[redacted]
MS	Microsoft
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
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
PIA	Privacy Impact Analysis
PIV	Personal Identity Verification
PL	Planning
POA&M	Plan of Action and Milestones
PUB	Publication
RA	Risk Assessment

RBST	Role Based Security Training
REV	Revision
RFQ	Request for Quotation
RM	Risk Management
RTO	Recovery Time Objective
SA	System and Services Acquisition
SC	System and Communication Protection
SI	System and Information Integrity
SP	Special Publication
[redacted]	[redacted]
SSP	System Security Plan
ST	Security and Awareness Training
[redacted]	[redacted]
[redacted]	[redacted]
US	United States
USC	United States Code
USGS	United States Geological Survey
[redacted]	[redacted]
[redacted]	[redacted]
WAN	Wide Area Network
[redacted]	[redacted]

Appendix III – Fiscal Year 2019 Recommendation Status

Below is a summary table of the FY19 FISMA report recommendations and the status as of October 31, 2020.

Table 1. FY2019 FISMA Report Recommendations and Status as of October 31, 2020.
26 of 27 Recommendations are Open[7]

Description	Status
1. [redacted] review and update the [redacted] to appropriately document and tailor the security control applicability and justification statements.	Open. Target Completion Date: December 31, 2020.
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.	Open. Target Completion Date: December 31, 2020.
3 [redacted] coordinate with DOI to design and implement a process to provide the department with [redacted] related information for the [redacted] system.	Open. Target Completion Date: December 30, 2020.
4. [redacted] continue to design and implement corrective actions identified in the [redacted] that addresses the protection of data at rest.	Open. Target Completion Date: October 30, 2020.
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]	Open. Target Completion Date: March 31, 2021.
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.	Open. Target Completion Date: March 31, 2021.
7. [redacted] design and implement a process for identifying all security patches applied to the [redacted] servers.	Open. Target Completion Date: March 31, 2021.
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.	Open. Target Completion Date: March 31, 2021.
9. Develop a solution for the [redacted] web server utilizing proper encryption mechanisms, such as [redacted] and renewal of the proper certificate.	Open. Target Completion Date: March 31, 2021.
10. [redacted] document procedures that require vulnerability scanning of [redacted] to be performed at least [redacted]	Open. Target Completion Date: December 31, 2020.

[7] Based on input from DOI, KPMG only included the status of FY19 recommendations in this report. KPMG further notes that 3 of 59 recommendation in the FY15 OIG FISMA report are open, 7 of 34 recommendations in the FY16 OIG FISMA report are open, 1 of 24 recommendations in the FY17 OIG FISMA report are open, and 7 of 25 recommendations in the FY18 OIG FISMA report are open.

11. [redacted] document and implement a solution that will provide the [redacted] with the functionality to perform vulnerability scanning across all components.	Open. Target Completion Date: December 31, 2020.
12. [redacted] document and implement procedures that require baseline configurations to be developed, documented, and monitored for compliance.	Open. Target Completion Date: December 31, 2020.
13. [redacted] document and implement a solution that will provide the [redacted] with the functionality to perform configuration baseline monitoring for baseline compliance.	Open. Target Completion Date: December 31, 2020.
14. [redacted] coordinate with DOI to design and implement a process to provide the department with [redacted] related information for the [redacted] system.	Open. Target Completion Date: December 31, 2020.
15. [redacted] develop and implement processes and technology that will support a security [redacted] 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.	Open. Target Completion Date: December 31, 2020.
16. [redacted] enforce established [redacted] patch implementation procedures that requires security patches be documented, tested, and approved through the [redacted] change management process.	Open. Target Completion Date: December 31, 2020.
17. [redacted] coordinate with DOI to design and implement a process to provide the department with [redacted] related information for the [redacted] system.	Open. Target Completion Date: December 31, 2020.
18. [redacted] ensure that the [redacted] is properly configured to perform credentialed vulnerability scanning on all [redacted] assets.	Open. Target Completion Date: December 31, 2020.
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 [redacted].	Open. Target Completion Date: December 31, 2020.
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]	Open. Target Completion Date: December 31, 2020.
21. [redacted] document and implement a formal process for reviewing the audit logs for potential misuse of privileged functions and actions.	Open. Target Completion Date: March 31, 2021.
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.	Open. Target Completion Date: March 31, 2021.
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.	Open. Target Completion Date: March 31, 2021.
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].	Open. Target Completion Date: March 31, 2021.

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.	Open. Target Completion Date: March 31, 2021.
26. [redacted] management ensure their [redacted] template aligns with the NIST SP 800- 34, Revision 1 key components for a Business Impact Assessment.	Closed. September 9, 2019.
27. [redacted] test the [redacted] in accordance with NIST requirements and DOI Security Control Standards using a functional test for the FIPS 199 moderate system.	Open. Target Completion Date: December 31, 2020.

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 2020 Questions for Inspectors General

The information included represents the Department of the Interior (DOI) responses to Department of Homeland Security's (DHS) FISMA 2020 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 2020 questions for the annual independent evaluation of DOI's security program. Within the context of the maturity model, Level 4, Managed and Measurable, is an effective level of security at the domain, function, and overall program level.

In accordance with the DHS FISMA reporting instructions, the ratings throughout the FISMA domains are determined by a simple majority, where the most frequent level across the metric questions serves as the domain rating. For example, if there are seven questions in a domain, and the agency receives Level 2: Defined ratings for three questions and Level 4: Managed and Measurable ratings for four questions, then the domain rating is Level 4: Managed and Measurable.

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 2020 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 Measurable	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.

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

We conducted a Performance Audit over the Department of the Interior's (DOI) information security program to determine the effectiveness of such program for the fiscal year (FY) ending September 30, 2020. 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 158 operational unclassified information systems, and we randomly selected 11 information systems across the Bureaus and Offices for the performance 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 in three of five function areas: Identify, Detect, and Recover. The Protect and Respond function areas were effective.

Weaknesses were noted in the FISMA domain areas of risk management, configuration management, data protection and privacy, information system continuous monitoring, and contingency planning domains.

KPMG assessed the cybersecurity Protect and Respond functions at Managed and Measurable (Level 4) and Identify, Detect, and Recover functions at Consistently Implemented (Level 3). Overall, KPMG assessed DOI's information security program and practices were 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 CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Maturity Level: Managed and Measurable (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.

2. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) 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 2020 CIO FISMA Metrics: 1.2

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. For mobile devices, the agency enforces the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period based on agency policy or guidance.

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: CA-7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; 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. For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization)

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 PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2020 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.

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, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?

Maturity Level: Ad Hoc (Level 1). Risk management policies, procedures, and strategy have not been fully defined, established, and communicated across the organization. The organization has not performed an organization-wide assessment of security and privacy risks to serve as an input to its risk management policies, procedures, and strategy.

Comments: 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.

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 (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 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. In addition, the organization employs a software assurance process for mobile applications.

Comments: The Department has implemented a security architecture at the Bureau, Office, and information system levels. However, the Bureaus and Offices did not integrate information and communication technology supply chain considerations in its information system development lifecycle.

DOI can improve and increase its maturity level, ensuring information security architectures are integrated with its systems development lifecycle, and DOI 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 M-19-03)?

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.

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.

Comments: DOI has implemented a Plan of Action and Milestone (POA&M) program. However, the Department has not developed and disseminated guidance to the Bureaus and Offices for the monitoring and analysis of qualitative and quantitative performance measures on the effectiveness of POA&M activities. Also, [redacted] did not consistently review and update POA&Ms in accordance with Departmental policies.

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.

Comments: DOI has not implemented a process to monitor its entity-wide risk responses to ensure that risk tolerances are maintained at an appropriate level. DOI can improve and increase its maturity level by implementing a process for monitoring the effectiveness of its entity-wide 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.

Comments: DOI has consistently communicated risks to stakeholders such as Bureau and Office Associate Chief Information Officers, Chief Information Security Officer, Authorizing Officials, and System Owners. Communication methods include email and minutes from various security working groups that meet periodically to discuss potential risks and threats to the department. In connection with the Department of Homeland Security (DHS) Continuous Diagnostic and Mitigation Program, DOI is developing the framework, 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.

Comments: However, DOI has not used qualitative and quantitative performance metrics to measure, report on, and monitor information security performance of contractor-operated systems and services.

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

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

Comments: 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.

Comments: The maturity level for the Risk Management function was assessed at Consistently Implemented (Level 3). One of 12 risk management metrics was accessed at Optimized (Level 5). Four of 12 risk management metrics were assessed at Managed and Measurable (Level 4). Six of 12 risk management metrics were assessed at Consistently Implemented (Level 3). One of 12 risk management metrics was assessed at Ad Hoc (Level 1).

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

Comments: No additional testing was performed beyond the above metrics. Based on the Consistently Implemented (Level 3) maturity level, the DOI Risk Management Program is not effective.

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.

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.

Comments: 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.

Comments: DOI has implemented policies and procedures for managing the configuration of its information systems. 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. Also, [redacted] did not effectively its configuration management plan for one information system. The information system configuration management plan did not fully document procedures to test, approve and implement system changes. [redacted] did not document a configuration management plan for one information system and [redacted] created a Plan of Action and Milestone (POA&M) to track the control weakness.

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 2020 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and 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.

Comments: DOI has implemented configuration management change control in accordance with Department Security Control Standards. However, [redacted] did not consistently implement procedures to ensure that baseline configurations are appropriately monitored for one information system in accordance with DOI security policies. [redacted] did not document a configuration management plan for one information system and [redacted] created a Plan of Action and Milestone (POA&M) to track the control weakness. Also, DOI is in the process of implementing an automated solution for application whitelisting.

18. To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; 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 on least functionality.

Comments: DOI has implemented software scanning capabilities and configuration management change control policies in accordance with Department Security Control Standards. However, [redacted] did not consistently implement procedures to ensure that baseline configurations are appropriately monitored and assessed for compliance for one information system. [redacted] did not document a configuration management plan for one information system and [redacted] created a POA&M to track the control weakness.

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, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?

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

20. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26).

Maturity Level: Managed and Measurable (Level 4). The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its [redacted] implementation remains flexible and that its policies and procedures, and information security program are adapting to meet the security capabilities in [redacted] 3.0, including the use of [redacted] requirements, as appropriate, for scenarios in which traffic may not be required to flow through a physical [redacted] access point. Further, the agency has developed a plan to update its internal network and system boundary policies to reflect OMB M-19-26, including guidance regarding [redacted] pilots, as appropriate.

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, CM-3 and CM-4; 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.

Comments: DOI has established and implemented change control policies and procedures. However, [redacted] and [redacted] did not document, test or approve system changes prior to implementation into production environment. [redacted] did not document a configuration management plan for one information system and [redacted] created a POA&M to track the control weakness.

DOI can improve and increase its maturity level by establishing and implementing procedures for testing and approving system changes and defining qualitative and quantitative performance measures on the effectiveness of its change control activities and ensuring data supporting the metric is obtained accurately, consistently, and in a reproducible format.

22.1 Please provide the assessed maturity level for the agency's Protect – Configuration Management function.

Comments: The maturity level for the Configuration Management function was assessed at Consistently Implemented (Level 3). Five of 8 configuration management metrics were assessed at Consistently Implemented (Level 3). Three of 8 configuration management metrics were assessed at Managed and Measurable (Level 4).

22.2 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?

Comments: No additional testing was performed beyond the above metrics. Based on the Consistently Implemented (Level 3) maturity level, 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.

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.

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

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.

Comments: [redacted] did not fully implement its personnel security program policies and procedures. [redacted] is working to remediate the weakness that was identified in a prior OIG FISMA audit. [redacted] did not document an identity and access management process for one information system and [redacted] created a POA&M to track the control weakness [redacted] did not ensure that all users were appropriately screened prior to gaining system access [redacted] did not establish an automated solution to centrally document, track, and share risk designations and screening information with necessary parties.

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

Comments: [redacted] did not fully implement its account management processes over one information system. [redacted] did not document an identity and access management process for one information system and [redacted] created a POA&M to track the control weakness. [redacted] did not ensure that all system users completed onboarding procedures and obtain approval prior to gaining system access. [redacted] did not implement automation to manage and review user access agreements for privileged and non-privileged users. [redacted] did not develop and implement procedures related to one information system for ensuring access agreements are completed for non-privileged and privileged users.

DOI can improve and increase its maturity level by ensuring that all user access agreements are maintained, and automation is used to manage and review user access agreements.

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 Measurable (Level 4). All non-privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.

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.

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: Ad-Hoc (Level 1). The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.

Comments: Six of 1l Bureaus and Offices - [redacted] - did not establish and implement procedures to review audit logs over privileged and non-privileged user activity. [redacted] effectively reviewed privileged and non-privileged user activity audit logs and implemented automation to disabled inactive accounts, as appropriate.

DOI can improve and increase its maturity level by implementing a process to ensure audit logs are reviewed for suspicious and unusual activity in accordance with DOI security policies.

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 allowing remote access and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.

32.1 Please provide the assessed maturity level for the agency's Protect – Identity and Access Management function.

Comments: The maturity level for the Identity and Access Management function was assessed at Managed and Measurable (Level 4). One of 9 identity and access management metrics was assessed at Ad-Hoc (Level 1). Two of 9 assessed at Consistently Implemented (Level 3). Six of 9 identity and access management metrics were assessed at Managed and Measurable (Level 4).

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

Comments: No additional testing was performed beyond the above metrics. Based on the Managed and Measurable (Level 4) maturity level, the Identity and Access Management 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, and reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs).

Comments: [redacted] did not review and update the privacy impact assessment in accordance with the DOI privacy policy. 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: Managed and Measurable (Level 4). The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization’s ISCM strategy.

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 3: Consistently Implemented. The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communication traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked.

Comments: DOI has implemented various technologies such as [redacted]. However, DOI has not developed qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses.

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.

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.

Comments: DOI tracks and monitors basic privacy awareness training and maintains a role-based privacy training self-certification module in the [redacted]. 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.

38.1 Please provide the assessed maturity level for the agency's Protect – Data Protection and Privacy function.

Comments: The maturity level for the Data Protection and Privacy function was assessed at Consistently Implemented (Level 3). Three of 5 Data Protection and Privacy metrics were assessed at Consistently Implemented (Level 3). Two of 5 Data Protection and Privacy metrics was assessed at Managed and Measurable (Level 4).

38.2 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?

Comments: No additional testing was performed beyond the above metrics. Based on the Consistently Implemented (Level 3) maturity level, the Data Protection and Privacy is not effective.

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 Measurable. 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.

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: Defined (Level 2). The organization has defined its processes for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment.

Comments: DOI did not complete its workforce assessment to identify the knowledge, skills, and specialized security training needed to support its security program. DOI can improve and increase its maturity level by completing the workforce assessment.

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 Measurable (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.

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 Measurable (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.

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: 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.

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.

45.1 Please provide the assessed maturity level for the agency's Protect – Security Training function.

Comments: The maturity level for the Security Training function was assessed at Managed and Measurable (Level 4). Five of 6 metrics were assessed at Managed and Measurable (Level 4). One of 6 was assessed at Defined (Level 2).

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

Comments: No additional testing was performed beyond the above metrics. Based on the Managed and Measurable (Level 4) maturity level, the Security Training function 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: Consistently Implemented (Level 3). The organization's ISCM strategy is consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM strategy.

Comments: DOI has established an information security continuous monitoring (ISCM) strategy. Five of 11 Bureaus and Offices, [redacted] monitor and analyze performance measures over their respective ISCM programs. However, six of 11 Bureaus and Offices, [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: Consistently Implemented (Level 3). 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.

Comments: DOI has established an information security continuous monitoring (ISCM) strategy. Five of 11 Bureaus and Offices, [redacted] monitor and analyze performance measures over their respective ISCM programs. However, six of 11 Bureaus and Offices - [redacted] - do not monitor and analyze qualitative and quantitative performance measures on the effectiveness of its ISCM strategy.

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: Consistently Implemented (Level 3). Individuals are performing the roles and responsibilities that have been defined across the organization.

Comments: DOI has established an information security continuous monitoring (ISCM) strategy. Five of 11 Bureaus and Offices, [redacted], monitor and analyze performance measures over their respective ISCM programs. However, six of 11 Bureaus and Offices - [redacted] - have not identified resources in a risk-based manner for stakeholders to effectively implement ISCM activities.

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 Measurable (Level 4). The organization utilizes the results of security control assessments and monitoring to maintain ongoing authorization of information systems.

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.

Comments: Four of 11 Bureaus and Offices, [redacted], integrate performance metrics on the effectiveness of its ISCM program to deliver situational awareness across the organization. However, five of 11 Bureaus and Offices, [redacted], do not integrate performance metrics on the effectiveness of its ISCM program to deliver situational awareness across the organization.

One of 11 Bureaus and Offices, [redacted] has not implemented procedures for integrate performance metrics on the effectiveness of its ISCM program to deliver situational awareness across the organization. [redacted] monitors ISCM performance of its cloud-based contractor managed system through the Federal Risk and Authorization Management Program (FedRAMP).

DOI can improve and increase its maturity level by ensuring its Bureaus and Offices integrate performance metrics on the effectiveness of its ISCM program to deliver situational awareness across the organization.

51.1 Please provide the assessed maturity level for the agency's Detect Information System Continuous Monitoring Function.

Comments: The maturity level for the ISCM function was assessed at Consistently Implemented (Level 3). Four of 5 ISCM metrics were assessed at Consistently Implemented (Level 3). One of 5 ISCM metrics assessed at Managed and Measurable (Level 4).

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

No additional testing was performed beyond the above metrics. Based on the Consistently Implemented (Level 3) maturity level, the ISCM program is not effective.

52. To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2020 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: Managed and Measurable (Level 4). The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

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 2020 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.

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: Consistently Implemented (Level 3). The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.

Comments: DOI can improve and increase its maturity level by designing and implementing profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.

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: Consistently Implemented (Level 3). The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations.

Comments: DOI has not designed and implemented processes to measure the impact of successful incidents that will allow the department to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.

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.

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.

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: Managed and Measurable (Level 4). The organization uses technologies for monitoring and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities

59.1 Please provide the assessed maturity level for the agency's Respond Incident Response Function.

Comments: The maturity level for the Incident Response function was assessed at Managed and Measurable (Level 4). Five of 7 incident response metrics were assessed at Managed and Measurable (Level 4). Two of 7 incident response metrics were assessed at Consistently Implemented (Level 3).

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

Comments: No additional testing was performed beyond the above metrics. Based on the Managed and Measurable (Level 4) maturity level, the Incident Response Program is 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.

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.

Comments: DOI has 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, DOI can improve and increase its maturity level by ensuring Bureaus and Offices document its information and communication technology (ICT) supply chain risks related to contingency planning activities.

As appropriate, apply ICT supply chain controls to alternate storage and processing sites, and consider alternate telecommunication service providers for the 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.

Comments: 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.

Comments: DOI consistently implemented information system contingency plans in accordance with DOI Security Control Standards. DOI has not defined performance metrics to measure the effectiveness of the contingency plans with information on the effectiveness of related plans, such as Bureau or Office continuity of operations plans or disaster recovery plans, to deliver situational awareness. [redacted] has not developed an information system contingency plan for one information system. [redacted] has taken corrective actions and developed a POA&M to monitor and track the control weakness.

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.

Comments: DOI has developed and implemented contingency planning policies and procedures to ensure information system contingency plan testing and exercises are performed in accordance with DOI Security Control Standards. However, [redacted] did not develop a contingency plan for one information system. [redacted] took corrective actions and developed a POA&M to track and monitor the control weakness. DOI can improve and increase its maturity level by employing automated mechanisms to 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.

Comments: DOI has consistently implemented information system backup and storage strategies as appropriate. However, one of 11 Bureaus and Offices, [redacted] did not geographically separate its primary and alternate processing sites. 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.

Due to the COVID-19 Pandemic, the Department of Homeland Security (DHS) cancelled the annual Eagle Horizon exercise, which is an exercise agency used to evaluate their recovery ability for mission essential functions and related information systems. DOI can improve and increase the maturity level by measuring the effectiveness of recovery activities and communicate results to relevant stakeholders and DOI to ensure that the data supports the metrics.

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

Comments: The maturity level for the Contingency Planning function was assessed at Consistently Implemented (Level 3). Six of 7 contingency planning metrics were assessed at Consistently Implemented (Level 3). One of 7 contingency planning metrics were assessed at Managed and Measurable (Level 4).

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

Comments: No additional testing was performed beyond the above metrics. Based on the Consistently Implemented (Level 3) maturity level, 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