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 2021

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

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

APR 28 2022

Memorandum

To: June Hartley
Acting 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 2021*
Report No. 2021-ITA-037

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) 2021. 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 2021 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 the DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-21-02, *Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements,* dated November 09, 2020. KPMG reviewed information security practices, policies, and procedures at the DOI's Office of the Chief Information Officer and the following 12 DOI bureaus and offices:

- Bureau of Indian Affairs
- Bureau of Land Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement
- Bureau of Ocean Energy Management

- U.S. Fish and Wildlife Service
- National Park Service
- Office of Inspector General
- Office of the Secretary
- Office of Surface Mining Reclamation and Enforcement
- Office of the Solicitor
- U.S. Geological Survey

To ensure the quality of the audit work, we:

- Reviewed KPMG's approach and planning of the audit
- Evaluated the auditors' qualifications and independence
- Monitored the audit's progress at key milestones
- 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, supply chain risk management, identity and access management, configuration management, data protection and privacy, information security continuous monitoring, incident response, and contingency planning. Using the FY 2021 Inspector General FISMA Report Metrics guidance and CyberScope results, KPMG determined that the DOI's information security program and practices were not effective because the majority of the Cybersecurity Functions were assessed as Consistently Implemented (Level 3). KPMG made 60 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, the Office of the Chief Information Officer concurred with all recommendations and established a target completion date for each corrective action.

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

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

Attachment

The United States Department of the Interior
Office of Inspector General
Federal Information Security Modernization Act of 2014
Fiscal Year 2021 Performance Audit

February 11, 2022

KPMG LLP
8350 Broad Street
McLean, Virginia 22102

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

February 11, 2022

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) 2021 Federal Information Security Modernization Act of 2014 (FISMA) Audit for unclassified information systems**.** We performed our work during the period of May 20 to September 30, 2021 and our results are as of November 9, 2021.

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 deficiencies and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our deficiencies 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 of our work for the year ending September 30, 2021 was to conduct an independent performance audit of the Department of the Interior's (DOI) information security program and practices related to the financial and nonfinancial related systems in accordance with the Federal Information Security Modernization Act (FISMA).

We tested select security controls identified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev) 4, and additional security program areas identified in the FY 2021 IG FISMA Reporting. We selected a sample of in-scope information systems distributed across 12 Bureaus and Offices. These Bureaus and Offices are: Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), Bureau of Ocean Energy Management (BOEM), 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 Solicitor (SOL), and the U.S. Geological Survey (USGS). At the conclusion of our test procedures, we aggregated the individual bureau and information system results by Cybersecurity Function and FISMA Metric Domain to produce results at the Department level.

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53, Rev 4. DOI has a security training program and no recommended improvements were identified. We identified needed improvements in the following FISMA Metric Domains: Risk Management (RM), Supply Chain Risk Management (SCRM), Identity and Access Management, (IAM), Configuration Management (CM), Data Protection and Privacy (DPP), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP).

Metrics are grouped into nine FISMA Metric Domains that are organized around the five Cybersecurity 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 RM and SCRM. The Protect Function area consists of CM, IAM, DPP, and Security Training (ST). The Detect Function area consists of ISCM. The Respond Function area consists of IR, and the Recover Function area consists of CP.

[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 results of testing.

Cybersecurity Framework Security Functions and FISMA Metric Domains	Summary of Results
1. Identify (RM and SCRM)	DOI established RM and SCRM programs; however, DOI did not ensure that: • Information system security plans (SSPs) are reviewed, updated, and approved annually at [redacted] and [redacted]. • Open Plan of Action and Milestones (POA&Ms) are reviewed and updated quarterly at [redacted], [redacted], [redacted], and [redacted]. • Security related policies and procedures are reviewed and updated at [redacted]. • Enterprise Architecture documentation that considers information security and the resulting risks are documented at [redacted]. • [redacted] mobile devices are compliant with approved operating systems at [redacted]. • User account management documentation is maintained and made it available for inspection at [redacted]. • Cybersecurity risk profiles are designed and documented at [redacted]. • Policies and procedures are developed for [redacted] component authenticity, anti-counterfeit training, and configuration control for component service and repair.

2. Protect (CM, IAM, and DPP)	DOI established CM, IAM, and DPP programs; however, DOI did not ensure that: • Information system security patches and updates are consistently tested, approved, and documented prior to implementation at [redacted]. • Security patches and system changes are documented and tested prior to implementation into production environment at [redacted] and [redacted]. • Security compliance scan policies are complete and accurate, and deviations from established baselines are documented and maintained at [redacted]. • POA&Ms for untimely remediation of failed compliance security checks are created at [redacted]. • Vulnerability assessment and compliance scan configurations are maintained at [redacted]. • Processes to remediate system vulnerabilities are operating as intended at [redacted]. • High risk vulnerabilities are remediated within [redacted] days at [redacted]. • CM documentation for baseline configuration, configuration change control, configuration settings, least functionality, information integrity, vulnerability scanning, and flaw remediation are maintained for the [redacted]. • [redacted] and [redacted] vulnerabilities were remediated in accordance with established timeframes for [redacted] at [redacted] and [redacted]. • [redacted], [redacted], and [redacted] vulnerabilities were remediated in accordance with established timeframes for [redacted] at [redacted] and [redacted]. • Privileged user access was reviewed and approved for one information system at [redacted]. • Personnel security procedures and related audit artifacts are maintained at [redacted]. • User account management procedures were adhered to at [redacted]. • A process to enforce completion of DOI required user access agreements, Rules of Behavior (ROB) forms, and security awareness training prior to provisioning user access was implemented at [redacted]. • Personnel security program and reinvestigation processes are adhered to at [redacted]. • Periodic reinvestigation of non-privileged users are conducted in accordance with investigation requirements at [redacted]. • A process to perform weekly audit log reviews to monitor privileged user activities are documented and implemented at [redacted]. • User access request forms, ROB forms, personnel risk designation documentation, and privacy agreements are maintained at [redacted] and [redacted]. • A system use notification or banner for publicly available information systems is defined and implemented at [redacted]. • Data protection and privacy controls and documentation to support the control environment are implemented and maintained at [redacted], [redacted], and [redacted].

3. Detect (ISCM)	DOI has established an ISCM program; however, DOI did not ensure that: • Results of security control self-assessments conducted weekly are maintained at the [redacted]. • Formal ISCM plans and the assessment of security and privacy controls are documented and implemented in accordance with DOI policy at [redacted]. • ISCM documentation, such as quarterly security control briefing reports provided to the Authorizing Official, for review are maintained at [redacted].
4. Respond (IR)	DOI has established an IR program; however, DOI did not ensure that: • IR program and associated security tool documentation is maintained at [redacted]. • All security incident tickets involving [redacted] are reported to the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT) [redacted].
5. Recover (CP)	DOI has established a CP program; however, DOI did not ensure that: • Information system contingency plans (ISCPs) are reviewed and updated to reflect current operations at [redacted]. • Information system backups are performed at [redacted]. • Functional CP tests or exercises for moderate information systems are performed at [redacted], [redacted], and [redacted]. • Alternate processing and storage sites are established at [redacted]. • Information system backups and business impact analysis (BIAs) are performed at [redacted]. • A contingency plan that supports all workstations within the [redacted] is documented. • A CP and business impact analysis was reviewed and updated in accordance with DOI requirements at [redacted].

Using the FY 2021 IG FISMA Report Metrics guidance and CyberScope results, we determined that DOI's information security program and practices were not effective because the majority of the Cybersecurity Functions were assessed as Consistently Implemented (Level 3).

We made 60 recommendations related to control deficiencies identified during our performance audit that, if effectively implemented by DOI, should strengthen DOI's information security program. Based on the control deficiencies identified, we made two additional recommendations to DOI.

The root causes that led to the control deficiencies identified as part of this performance audit may contribute to control deficiencies for other systems outside of the scope of this audit. DOI should consider and, if deemed necessary, apply these recommendations to its entire universe of systems.

Furthermore, DOI should implement a robust monitoring capability to continually assess the cybersecurity state of these information systems to include a process to hold Bureaus and Offices accountable for identified control gaps.

This 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 FY 2020 recommendations, Appendix IV lists the NIST SP 800-53 security controls cross-referenced to the Cybersecurity Framework, and Appendix V provides the responses to the FY 2021 IG FISMA Reporting Metrics.

We were 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. We caution 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 12 Bureaus and Offices are included within the scope of the Office of the Inspector General's (OIG) Federal Information Security Modernization Act of 2014 (FISMA) performance audit for Fiscal Year (FY) 2021:

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

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

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

8 The **Office of Inspector General (OIG)** provides independent oversight and promote excellence, integrity, and accountability within the programs, operations, and management of the DOI.

9 The **Office of the Secretary (OS)** is primarily responsible for providing quality services and efficient solutions to meet DOI business needs.

10 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, to assure the land is restored to beneficial use following mining, and to mitigate the effects of past mining by aggressively pursuing reclamation of abandoned coalmines.

11 The **Office of the Solicitor (SOL)** performs the legal work for the DOI and manages the Departmental Ethics Office and the Departmental Freedom of Information Act (FOIA) Office.

12 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) oversees the cybersecurity management program for the Department. The Chief Information Officer (CIO) leads the OCIO and is responsible for the management and oversight of the Interior's information management and technology (IMT) portfolio; the Department CIO reports to the Department Secretary and receives operational guidance and support from the Assistant Secretary – Policy, Management and Budget through the Deputy Assistant Secretary – Technology, Information, and Business Services.

The Deputy CIO (Program Management Division) 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), also the Director of Cybersecurity (CSD) within the OCIO, 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.

Each Bureau and Office Support Division has 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) represents 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

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 FY 2021 FISMA Reporting Metrics were aligned with the five function areas in the National Institute of Standards and Technology (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 (IG) with guidance for assessing the maturity of controls to address those risks.

Objective, Scope, and Methodology

The audit objective of our work for the year ending September 30, 2021 was to conduct an independent performance audit of DOI's information security program and practices related to the financial and nonfinancial related systems in accordance with FISMA.

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 FY2021 OIG FISMA Reporting Metrics; and
- An inspection of the information security practices, policies, and procedures in use across 12 Bureaus and Offices identified by the DOI OIG, specifically BIA, BLM, BOR, BSEE, BOEM, FWS, NPS, OIG, OS, OSMRE, SOL, 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 were generally consistent with FISMA.

Step B: Assessment of the implementation of select security controls from the NIST SP 800-53, Rev 4 – During this step, we assessed the implementation of a selection of security controls from the NIST SP 800-53, Rev 4 for our representative subset of DOI's information systems.[3] The controls selected addressed areas covered by the FY2021 IG FISMA Reporting Metrics.

[3] The OIG judgmentally selected 12 of 160 unclassified operational systems recorded in the Departments official repository, the Cyber Security Assessment and Management tool (CSAM). The representative subset includes Major Applications and General Support Systems with FIPS 199 security categorizations of "Low" and "Moderate," The Federal Information Processing Standard (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	BOEM	[redacted]	[redacted]	[redacted]
6	FWS	[redacted]	[redacted]	[redacted]
7	NPS	[redacted]	[redacted]	[redacted]
8	OIG	[redacted]	[redacted]	[redacted]
9	OS	[redacted]	[redacted]	[redacted]
10	OSMRE	[redacted]	[redacted]	[redacted]
11	SOL	[redacted]	[redacted]	[redacted]
12	USGS	[redacted]	[redacted]	[redacted]

Results of Review

Our procedures identified improvements needed in the five Cybersecurity Function areas: Identify (Risk Management and Supply Chain Risk Management), Protect (Configuration Management, Identity and Access Management, and Data Protection and Privacy), Detect (Information System Continuous Monitoring), Respond (Incident Response), and Recover (Contingency Planning).

In the following section, a summary of deficiencies identified during our performance audit is provided.

1. Identify Function: Implementation of the RM Program.

The table below lists deficiencies in the RM FISMA Metric Domain.

FISMA Metric Domain	Summary of Deficiencies
RM	DOI established a RM program; however, DOI did not ensure that: • Information system security plans (SSPs) are reviewed, updated, and approved annually at [redacted] and [redacted]. • Open Plan of Action and Milestones (POA&Ms) are reviewed and updated quarterly at [redacted], [redacted], [redacted], and [redacted]. • Security related policies and procedures are reviewed and updated at [redacted]. • [redacted] documentation that considers information security and the resulting risks are documented at [redacted]. • [redacted] mobile devices are compliant with the approved operating system at [redacted]. • User account management documentation is maintained and made it available for inspection at [redacted]. • Cybersecurity risk profiles are designed and documented at [redacted].

We performed the following procedures and noted the following deficiencies in 5 of 12 Bureaus' and Offices' risk management programs: [redacted], [redacted], [redacted], [redacted], and [redacted].

[redacted]:

We obtained and inspected the [redacted] SSP, dated June 24, 2019, and noted that the SSP was not reviewed, updated, or approved within the required annual frequency in accordance with DOI security control standards.

We inspected the open POA&Ms and determined that of 18 open POA&Ms selected for testing, 9 were not consistently reviewed or updated, or rationale supporting delayed milestones was not maintained.

[redacted]:

We inspected [redacted] cybersecurity policies and procedures and determined several policies and procedures were not reviewed or updated within the required [redacted] in accordance with DOI requirements.

The following eight documents were last reviewed or updated in July and December 2018: [redacted]

We inquired of [redacted] management and were informed that management had not developed an [redacted], which considers information security and the resulting risks to the Bureau and DOI operations, assets, individuals and other organizations, as required by DOI Security Control Standards.

We found that [redacted] manages and provides oversight to all [redacted] information systems, including the [redacted] information system. We inspected the one open [redacted] POA&M and noted it was not updated with milestones, delay justifications, and other evidence to validate management reviewed the POA&M on a quarterly basis in accordance with DOI policy.

[redacted]:

We inquired of management and inspected policies and procedures related to POA&Ms and determined a POA&M process was implemented. We randomly selected 5 of 16 open Bureau level POA&Ms and 5 of 42 open [redacted] POA&Ms listed in the Cyber Security Assessment and Management (CSAM) tool to determine whether POA&Ms are appropriately reviewed or updated. We determined that 9 of 10 selected POA&Ms were not updated quarterly with new milestones or that delay justifications were not documented. While the POA&Ms were reviewed on a quarterly basis, we determined progress to closure was not appropriately documented.

We obtained and inspected the [redacted] mobile device inventory within [redacted], the Mobile Device Management (MDM) solution. Also, we obtained and inspected the DOI policy: [redacted], dated November 2, 2020 and determined that the Department required all DOI [redacted] mobile devices to use the minimum operating system version of [redacted] by December 1, 2020.

We determined that as of August 26, 2021, 288 of 5,324 (5%) [redacted] mobile devices were not compliant with the minimum required operating system version of [redacted]. Specifically, we noted the following deficiencies in the table below:

Table 2. Number of mobile devices not compliant.

Number of Mobile Devices Not Compliant	Operating System Versions
3	[redacted]
103	[redacted]
182	[redacted]

Additionally, we were informed that a risk acceptance or Weaknesses Completion Verification Form (WCVF) to document and accept the risk of using outdated operating systems was not documented.

[redacted]:

We inquired of [redacted] management and requested audit documentation for review and inspection to support testing over the RM FISMA Metric Domain. Audit evidence, such as system generated lists of users, user access request forms, and evidence of account management reviews were not available for inspection; therefore, Access Control (AC) 2, Account Management was determined to be ineffective.

[redacted] management continued to collect artifacts after established audit document submission due dates; however, we were unable to review and inspect the artifacts after such dates.

[redacted]:

We inquired of [redacted] management to determine whether the office documents and maintains its cybersecurity risk profile and were informed that a cybersecurity risk profile was not in place.

We randomly selected and inspected 6 of 18 open [redacted] POA&Ms to determine whether they were reviewed or updated. We noted that 4 of 6 open POA&Ms were not updated quarterly with new milestones or that delay justifications were not documented.

We obtained and inspected the [redacted] SSP, dated May 2015, and noted the plan was not reviewed, updated, and approved within the required annual frequency.

OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, states the following:

> B. Risk Profiles
>
> Agencies must maintain a risk profile. The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives. The risk profile differs from a risk register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks. The risk profile must consider risks from a portfolio perspective and be approved by an Agency's RMC or equivalent. Additionally, the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats).
>
> The development of an Agency risk profile:
>
> • encourages open and candid conversations about risks facing an organization at all levels;
>
> • facilitates the ranking of risk priorities (in particular to identify and escalate the most significant risks of which senior management should be aware);
>
> • captures the reasons for decisions made about risk tolerances;
>
> • facilitates recording of the way in which it is decided to address risk;
>
> • allows leadership at all levels to understand the overall risk profile and how their areas of particular responsibility fit into it; and
>
> • facilitates the review and regular monitoring of risks.

Agencies have discretion in terms of the appropriate content and format for their risk profiles; however, in general risk profiles should include the following seven components:

1. Identification of Objectives
2. Identification of Risk
3. Inherent Risk Assessment
4. Current Risk Response
5. Residual Risk Assessment
6. Proposed Risk Response
7. Proposed Action Category

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2 Account Management, states:

The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-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 [Assignment: organization-defined frequency]; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

NIST SP 800-53, Rev. 4, *Information Security Program Plan*, PM-1 states: The organization:
b. Reviews the organization-wide information security program plan [Assignment: organization defined frequency];

DOI Security Control Standard Security Assessment and Authorization (CA), version 4.1, CA-1 Security Assessment and Authorization Policy and Procedures, states:

> The organization:
> a. Develops, documents, and disseminates to all relevant parties:
> 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
> b. Reviews and updates as needed the current:
> 1. Security assessment and authorization policy, at [redacted]; and
> 2. Security assessment and authorization procedures, at [redacted] years.

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

> 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.

DOI Security Control Standard Planning, PL-2 System Security Plan, states:

> The organization:
>
> a. Develops a security plan for the information system that:
> 1. Is consistent with the organization's enterprise architecture;
> 2. Explicitly defines the authorization boundary for the system;
> 3. Describes the operational context of the information system in terms of missions and business processes;
> 4. Provides the security categorization of the information system including supporting rationale;
> 5. Describes the operational environment for the information system and relationships with or connections to other information systems;
> 6. Provides an overview of the security requirements for the system;
> 7. Identifies any relevant overlays, if applicable;
> 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
> 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
> b. Distributes copies of the security plan and communicates subsequent changes to the plan to all relevant parties;
> c. Reviews the security plan for the information system at least annually;
> d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
> e. Protects the security plan from unauthorized disclosure and modification.

DOI Security Control Standard Program Management (PM), version 4.1, PM-7 [redacted], states: "The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation."

DOI Security Control Standard PM, version 4.1, PM-8 Critical Infrastructure Plan, states: "The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan."

United States Department of the Interior Office of the Secretary, Subject: [redacted] states:

[redacted]

[redacted]:

[redacted] management has not prioritized the review, update, or approval of the SSP.

[redacted] management reviews POA&MS quarterly with the Authorizing Official (AO); however, it has not prioritized updating POA&M specific milestones when milestones are missed or delayed.

[redacted]:

[redacted] management stated that it did not review and approve its policy and procedure documents within the [redacted] interval due to a breakdown in the [redacted]. The bureau leverages its [redacted] to facilitate its on-going authorization and review process. The [redacted] contains a trigger log that contains prerequisites for policy and procedure review. The trigger log did not include the [redacted] review requirement and, as a result, management was not alerted to review and update policy and procedure documents within the frequency prescribed by the DOI Security Control Standards.

[redacted] management stated that it has not placed an emphasis on developing an [redacted] with consideration for information security due to other priorities.

[redacted] management informed us that, due to human error, management did not review and update the [redacted] POA&M on a quarterly basis.

[redacted]:

[redacted] and [redacted] management did not consistently prioritize the review or update of POA&Ms.

We were informed that, in response to the Coronavirus Disease 2019 (COVID-19)[4] pandemic, [redacted] management prioritized maintaining mobile device service and connectivity for end-users due to the remote work environment.

[4] Coronavirus disease (COVID-19) is an infectious disease.

[redacted]:

Due to lack of internal communications following change in personnel assignments within the [redacted], management was unable to provide sufficient audit documentation within the period designated by the auditors.

[redacted]:

We were informed that due to inadequate staffing and resource prioritization, [redacted] did not implement a process to create, maintain, and update a risk profile in accordance with OMB A-123.

We were informed [redacted] did not implement a process to periodically review and update POA&Ms due to inadequate staffing and resource prioritization.

[redacted] management did not prioritize the review, update, or approval of the SSP due to inadequate staffing and resource prioritization.

[redacted]:

Failing to review and approve the SSP could lead to the plan becoming ineffective in addressing changes to information systems that could lead to inappropriate use and exposure of the system and its data.

Not reviewing and updating POA&Ms periodically could lead to delays in remediating and resolving known risks, control deficiencies, and vulnerabilities within the security boundary of [redacted], which could in turn result in exploited vulnerabilities hindering the operations, thereby impacting the data within the system.

[redacted]:

Bureau-wide information security policies and procedures provide guidance over controls implemented for information systems. Outdated documentation can lead to a misunderstanding of the information system control environment. This in turn increases the risk of improper controls implementation, thereby exposing [redacted] systems to vulnerabilities or security risks.

The lack of an [redacted] may result in security considerations not being addressed within the system development life cycle, which could lead to inconsistencies in the implementation of [redacted]'s information security strategies.

The failure to periodically review and update POA&Ms could lead to delays in remediating and resolving known risks, control deficiencies, and vulnerabilities within the security boundary of [redacted], which could result in exploited vulnerabilities that hinder operations and/or impact the data within the system.

[redacted]:

The failure to periodically review and update POA&Ms could lead to delays in remediating and resolving known risks, control deficiencies, and vulnerabilities within the security boundary of [redacted], which could result in exploited vulnerabilities that hinder operations and/or impact the data within the system.

An outdated operating system increases the risks of compromised mobile devices, which could subject these devices to exposure and/or loss of data, lack of system availability, and other malicious and unauthorized activities.

[redacted]:

Without audit documentation to review and inspect, the risk of not identifying control gaps in management's processes and procedures is significantly increased. Consequently, potential vulnerabilities and control weaknesses may not be identified, thereby exposing the system and organization to various risks, such as system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] to fulfill its mission requirements.

[redacted]:

Without the ability to identify and prioritize cybersecurity risk profiles and identify response actions to mitigate risk around the environment, such risk may not be properly identified, prioritized, or mitigated, which could leave the [redacted]'s systems and data exposed to unauthorized access, disclosure, and modification.

The failure to periodically review and update POA&Ms could lead to delays in remediating and resolving known risks, control deficiencies, and vulnerabilities within the security boundary of [redacted], which could result in exploited vulnerabilities that hinder operations and/or impact the data within the system.

Failing to periodically review, update and approve the SSP could lead to the plan becoming ineffective in addressing changes to information systems, which could lead to inappropriate use and exposure of the system and its data.

We recommend [redacted]:

1. Ensure that [redacted] management implements procedures enforcing the requirement to review, update, and approve the SSP [redacted] in accordance with DOI security control standards.
2. Enforce established procedures to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

We recommend [redacted]:

3. Update policy and procedure review requirements to ensure [redacted] cybersecurity policies and procedures are reviewed within the [redacted] interval in accordance with DOI Security Control Standards.
4. Review and update the eight outdated policy and procedures documents: [redacted] *Control* [redacted]. Further, ensure such documentation is reviewed and updated on a going-forward periodic basis in accordance with DOI Security Control Standards.
5. Document, implement, and maintain both a current state and future state [redacted] that follows DOI Security Standards. The [redacted] should consider information security and the resulting risk to [redacted] and DOI operations, assets, and individuals.
6. Enhance the established POA&M review process to ensure that all open POA&Ms are regularly and consistently reviewed to ensure that they are updated and remediated per the defined date(s) established within the POA&M.
7. Review [redacted] POA&M [redacted] and update the POA&M's attributes accordingly.

We recommend [redacted]:

8. Implement a process to consistently ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.
9. Ensure all mobile devices are operating the minimum approved [redacted] baseline in accordance with DOI policy or obtain a formal policy exception from the DOI Chief Information Security Officer.

We recommend [redacted]:

10. Design and implement a process to ensure access control documentation is retained to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 4.

We recommend [redacted]:

11. Implement a process to create and periodically update the cybersecurity risk profile in accordance with OMB A-123 requirements.
12. Implement a process to ensure all POA&Ms are appropriately reviewed and updated in accordance with DOI policy requirements.
13. Implement procedures that ensure the [redacted] SSP is reviewed, updated, and approved at least annually in accordance with DOI security control standards.

2. Identify Function: [redacted] Program.

The table below lists deficiencies in the [redacted] FISMA Metric domain.

FISMA Metric Domain	Summary of Deficiency
[redacted]	DOI did not develop policies and procedures for [redacted] component authenticity, anti-counterfeit training, and configuration control for component service and repair.

We performed the following procedures and noted deficiencies associated with DOI's supply [redacted] program. We inquired of DOI [redacted] management to determine whether a [redacted] program was established and whether controls are implemented throughout the Department. We were informed that DOI had not developed policies and procedures for [redacted] component authenticity, anti-counterfeit training, and configuration control for component service and repair; consequently, we determined that none of the 12 Bureaus and Offices implemented a [redacted] program.

Office of Management and Budget (OMB) Circular No. A-130, *Managing Information as a Strategic Resource*, Appendix I to OMB Circular A-130, Responsibilities for Protecting and Managing Federal Information Resources states that:

> The organization:
> a. Shall develop, implement, document, maintain, and oversee agency-wide information security and privacy programs including people, processes, and technologies to:
>
> > 1. Implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle.

[redacted]:

We were informed that [redacted] did not prioritize the development of policies and procedures to support [redacted] component authenticity, anti-counterfeit training, and configuration control activities for component service and repair.

[redacted]:

Without implementing [redacted] policies and procedures, there is an increased risk of compromise to the Department's integrity, security, quality and resilience, and its products and services. In addition, the Department could experience threats related to issues for counterfeits, unauthorized and/or inappropriate production, tampering, theft, insertion of malicious software and hardware as well as poor manufacturing and development practices in the [redacted].

We recommend DOI:

14. Enhance the established [redacted] policies and procedures to include processes over supply chain component authenticity, anti-counterfeit training, and configuration control for component service and repair.

3. Protect Function: Implementation of the CM Program.

The table below lists deficiencies in the CM program.

FISMA Metric Domain	Summary of Deficiencies
CM	DOI established a CM program; however, DOI did not ensure that: • Information system security patches and updates are consistently tested, approved, and documented prior to implementation at [redacted]. • Security patches and system changes are documented and tested prior to implementation into production environment at [redacted] and [redacted]. • Security compliance scan policies are complete and accurate, and deviations from established baselines are documented and maintained at [redacted]. • POA&Ms for untimely remediation of failed compliance security checks are created at [redacted]. • Vulnerability assessment and compliance scan configurations are maintained at [redacted]. • Processes to remediate system vulnerabilities are operating as intended at [redacted]. • High risk vulnerabilities are remediated within [redacted] at [redacted]. • CM documentation for baseline configuration, configuration change control, configuration settings, least functionality, information integrity, vulnerability scanning, and flaw remediation are maintained for the [redacted] system. • [redacted] and [redacted] vulnerabilities were remediated in accordance with established timeframes for [redacted] at [redacted] and [redacted]. • [redacted], [redacted], and [redacted] vulnerabilities were remediated in accordance with established timeframes for [redacted] at [redacted] and [redacted].

We performed the following procedures and noted the following deficiencies in 6 of 12 Bureaus' and Offices' CM programs: [redacted], [redacted], [redacted], [redacted], [redacted], and [redacted].

[redacted]:

We randomly selected [redacted] connected to the DOI network and performed vulnerability security scans to determine whether patch and configuration management practices were effective and whether critical, high, and medium risk vulnerabilities were present.

[redacted] and [redacted] vulnerabilities were not remediated timely in accordance with DOI security control standards. Specifically, we noted the following:

[redacted]

We subsequently inquired of management and inspected system records and determined that management remediated the [redacted] vulnerabilities upon notification of this deficiency.

[redacted]:

We inquired of [redacted] management to determine whether security-related patches are tested and approved prior to implementation and subsequently documented and retained. We were informed that evidence of testing and approvals were not documented and maintained for [redacted] security patches, as required by the [redacted] SSP and [redacted] Plan policies and procedures.

[redacted]:

We inquired of [redacted] management and inspected Request for Change (RFC) artifacts to determine whether a CM program was implemented and working as intended. Specifically, we selected and inspected 5 of 16 security patches to determine whether security patches were approved and tested prior to implementation. We noted that for all five selected security patches, management did not document results of security patch testing in RFCs as required by policy.

Also, we selected and inspected documentation associated with 2 of 11 information system changes, which included hardware configuration, software configuration changes, and system upgrades to the [redacted] system. We noted that for one of the two selected system changes, management did not document the testing of the system changes within an RFC.

We obtained and inspected 10 baseline compliance scans from the [redacted] We compared the sampled server compliance scans to the [redacted] checklist approved by [redacted] management as the relevant Standard Technical Implementation Guide (STIG) to verify audit checks were being scanned. We noted that 67 audit checks on the [redacted] checklist were not included in the compliance scan policy. As such, we determined the [redacted] compliance scans to be incomplete and inconsistent with the [redacted] STIG.

Additionally, we noted that as of August 9, 2021, 121 failed audit checks from compliance scans performed during the period February 2021 to May 2021 were unresolved, and management did not obtain formal risk acceptance or create POA&Ms for associated non-compliant configurations.

We inquired of [redacted] management and requested audit documentation in support of testing over the CM domain area. We were informed that audit evidence, such as [redacted], was unavailable for inspection.

We tested [redacted][5] servers connected to the DOI network and performed vulnerability security scans to determine whether patch and CM practices were effective and whether critical, high, and medium risk vulnerabilities were present.

[redacted], [redacted], and [redacted] vulnerabilities were not remediated timely in accordance with DOI security control standards. Specifically, we found the following:

[redacted]

[5] [redacted].

[redacted].

KPMG was informed by [redacted] management that actions were taken to prevent the [redacted] ability to access the Internet to limit its exposure. Also, the device monitoring functionality within [redacted] management monitored the [redacted] activity during the repurposed period. We conducted technical security testing to confirm the [redacted] ability to access the Internet.

We inspected system records and determined that management remediated [redacted], [redacted], and [redacted] vulnerabilities by [redacted] on October 26, 2021.

[redacted]:

We inspected the [redacted] patch management process to determine whether security patches and updates were approved and tested prior to being implemented. We found that because security patches were [redacted] to the [redacted], such patches were not tested prior to implementation as required by DOI Security Control Standards.

We also noted that [redacted] security patches were [redacted]. We were informed that [redacted] management did not maintain documentation to support management's rationale or risk assessment supporting the [redacted]. Due to the lack of approval documentation, we determined that security patches were not adequately reviewed or approved prior to being implemented.

Additionally, none of the 15 [redacted] patches inspected were appropriately tested and approved prior to being implemented in accordance with DOI Security control standards.

[redacted] management was unable to provide evidence of review for 1 of 15 randomly selected [redacted].

[redacted] management omitted the [redacted] system from its [redacted] "Vulnerability Management Sync Up" meeting, which is used by the bureau to oversee and monitor system-level vulnerability status and vulnerability remediation efforts.

[redacted] management did not remediate [redacted] vulnerabilities within the established timeframes. We compared results of a judgmental selection of daily [redacted] to each other to determine whether reports indicated the timely resolution of identified vulnerabilities. Based on these comparisons, we determined that management did not remediate the [redacted] vulnerabilities within [redacted] vulnerabilities, as summarized in the Table 3 below:

Table 3. Number of [redacted] Vulnerabilities Not Remediated in a Timely Manner

	[redacted] Vulnerabilities		[redacted] Vulnerabilities	
Scan Comparison Dates	**Vulnerabilities Not Remediated**	**Days Overdue**	**Vulnerabilities Not Remediated**	**Days Overdue**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Additionally, a POA&M, Weakness Completion Verification Form (WCVF), or risk acceptance form was not completed to address the overdue [redacted] vulnerabilities.

[redacted]:

We obtained and inspected five [redacted] vulnerability monthly scan reports from January 2021 through May 2021 for the [redacted] to determine whether all [redacted] vulnerabilities were remediated within [redacted] from date vulnerability was first identified.

We noted [redacted] vulnerabilities related to the [redacted] was not remediated in a timely manner. We inquired of management and inspected system records and determined that on [redacted], 2021, [redacted] released an interim security patch, and, on [redacted], 2021, the patch was installed. However, we determined that the [redacted] vulnerability was not remediated within [redacted] in accordance with DOI Security Control Standards.

Additionally, we conducted independent technical security testing to determine whether critical, high, and medium risks vulnerabilities were present. We noted that configuration management practices such as the implementation of security patches and system updates were not consistently performed on either of the two [redacted] servers. We subsequently inquired of management and inspected system records and determined that management remediated the vulnerabilities upon notification of this deficiency.

[redacted]:

We inquired of [redacted] management and requested audit documentation for inspection to support testing over the CM FISMA Metric Domain.

Audit evidence was not available for inspection; therefore, the following NIST SP 800-53, Rev 4, configuration management, risk assessment and system and information integrity security controls were determined to be ineffective:

- Configuration Management (CM) 2: Baseline Configuration
- CM-3: Configuration Change Control
- CM-6: Configuration Settings
- CM-7: Least Functionality
- CM-8: Information System Component Inventory
- Risk Assessment (RA) 5: Vulnerability Scanning
- System and Information Integrity (SI) 2: Flaw Remediation

The [redacted] continued to collect artifacts after established audit document submission due dates to provide evidence; however, we were unable to review and inspect the artifacts after such dates.

We randomly selected [redacted] servers connected to the DOI network and performed vulnerability security scans to determine whether patch and configuration management practices were effective and whether critical, high, and medium risk vulnerabilities were present.

Upon analysis of DOI's [redacted] vulnerability security scan results, we determined that two of three [redacted] servers selected for testing possessed [redacted] vulnerabilities. In addition, a [redacted] vulnerability existed for more than [redacted] after first detection.

[redacted] vulnerabilities were not remediated timely in accordance with DOI security control standards. Specifically, we noted the following:

[redacted]

We subsequently inquired of management and inspected system records and determined that management remediated the [redacted] vulnerability upon notification of this deficiency.

We randomly selected three [redacted][6] servers connected to the DOI network and performed vulnerability security scans to determine whether patch and CM practices were effective and whether critical, high, and medium risk vulnerabilities were present.

Upon analysis of DOI's [redacted] vulnerability security scan results, we determined that all three [redacted] servers were vulnerable to [redacted] vulnerabilities and that a [redacted] vulnerability existed for more than [redacted].

[redacted] vulnerabilities were not remediated timely in accordance with DOI Security Control Standards. Specifically, we found the following:

[redacted]

[6] [redacted].
[7] [redacted].

GAO *Standards for Internal Control in the Federal Government*, states:

> 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.
>
> 3.11 - Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

DOI Security Control Standard System Information Integrity, version 4.1, Control SI-2 Applicability, states:

> 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,* [redacted], of the release of the updates; and
> d. Incorporates flaw remediation into the organizational configuration management process.

DOI Security Control Standard Configuration Management, version 4.1, Control CM-3, states:

> 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.

DOI Security Control Standards Configuration Management version 4.1, CM-3(2), states:

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

DOI Security Control Standards Risk Management version 4.2, RA-5 Vulnerability Scanning Control: The organization:

> a. Scans for vulnerabilities in the information system and hosted applications in accordance with DOI's Scanning Policy, and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    i. Enumerating platforms, software flaws, and improper configurations;
    ii. Formatting checklists and test procedures; and
    iii. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities to Internet-accessible systems within [redacted] for critical vulnerabilities, [redacted] for critical vulnerabilities on non-Internet accessible systems, [redacted] for high risk/important vulnerabilities on all systems, and within [redacted] for moderate risk vulnerabilities on all systems in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with the CDM program and [redacted] personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

CM-6 Configuration Settings

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

NIST SP 800-53, Rev. 4, CM-2 Baseline Configuration, states:

The organization:
a. Develops, documents, and maintains under configuration control, a current baseline configuration of the system; and
b. Reviews and updates the baseline configuration of the system:
    1. [Assignment: organization-defined frequency];
    2. When required due to [Assignment: organization-defined circumstances]; and
    3. When system components are installed or upgraded.

NIST SP 800-53, Rev. 4, CM-7 Least Functionality, states:
The organization:
a. Configures the information system to provide only essential capabilities; and

b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

NIST SP 800-53, Rev. 4, CM-8 Information System Component Inventory, states:

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

1. Accurately reflects the current information system;

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

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

4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and

b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

[redacted], [redacted], states:

[redacted]

[redacted].

[redacted]

[redacted] states:

F. [redacted] shall implement processes incorporating the following parameters to ensure the timely remediation of vulnerabilities:

[redacted]

[redacted], states:

[redacted]

[redacted]:

[redacted] did not prioritize adherence to DOI Security Control Standards associated with the performance of security patch and configuration remediation efforts in response to previous vulnerability scans conducted for [redacted] connected to the DOI network or create a POA&M to document corrective actions.

[redacted]:

[redacted] management did not prioritize the requirement to document the approval and testing of security related patches before implementation.

[redacted]:

[redacted] management did not prioritize the requirement to maintain audit evidence that support system flaw remediation processes.

[redacted] management did not prioritize the requirement to identify and document STIG policy exceptions and deviations. We inquired of management and were informed that management did not document policy exceptions or deviations from the STIG for items that are not applicable or are risk accepted to explain the 67 missing checks.

[redacted] management did not adhere to DOI security policies or maintain audit evidence to support activities related to the [redacted] vulnerability scan tool.

[redacted]:

[redacted] management informed us that it did not prioritize the institution of procedural requirements to retain supporting documentation evidencing the review, testing, and approval of security patches.

[redacted] management's bi-weekly "Vulnerability Management Sync-Up" meetings only included systems that reside on [redacted]. [redacted] system does not reside on the [redacted] and, as a result, it was not being included in management's bi-weekly "Vulnerability Management Sync-Up" meetings. Therefore, the [redacted] system's vulnerability status was not consistently communicated to bureau management and vulnerabilities were not addressed timely.

Additionally, [redacted] management did not prioritize the enforcement of requirements to document its review of vulnerability scan results or the remediation efforts that resulted from the review.

[redacted]:

[redacted] management was not aware that the interim patch, which was released outside the standard patch cycle, did not include all [redacted] security patch information from previous patches.

[redacted] management informed KPMG that because of the current volume of analysis and testing required for patching, the deployment of patch management coordination efforts between separate entities within [redacted] led to challenges in remediating documented IT security vulnerabilities in a timely manner.

[redacted]:

Due to lack of internal communications following change in personnel assignments within [redacted], [redacted] management was unable to provide sufficient audit documentation within the period designated by the auditors.

DOI did not prioritize the enforcement of requirements to complete security patch and configuration remediation efforts in a timely manner.

[redacted]: [redacted] did not prioritize the enforcement of requirements to complete security patch and configuration remediation efforts in a timely manner or create a POA&M to document its corrective actions.

[redacted]:

Without remediating [redacted] vulnerabilities on a timely basis, [redacted] cannot ensure the security and compliance of the system's computing environment. System misconfigurations and vulnerabilities could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] to fulfill its mission requirements.

[redacted]:

Security patches that are not adequately tested and approved prior to implementation could result in critical system errors, compromises to systems and data, and disruption of services.

[redacted]:

Critical errors, compromises of systems and data, and/or disruption of services could occur if patches and system changes are not tested and the change process is not fully followed, documented, and retained, as required by DOI Security Control Standards.

Failing to properly monitor baseline configurations and remediate instances of non-compliance increase the risk that key security controls are ineffective/not implemented and the system is vulnerable to internal and external threats or attacks.

A lack of available audit evidence prevents internal and external parties from being able to complete required audits of [redacted]'s controls, which increases the risk that gaps in management's controls and processes are not identified and addresses, thereby exposing the system and data to confidentiality, integrity, and availability risks.

[redacted]:

A lack of patch testing and approval could result in critical system errors and disruption of service. Information system vulnerabilities that are not remediated timely leave the system exposed to compromise by both external and internal threat sources.

[redacted]:

Without remediating [redacted] vulnerabilities on a timely basis, [redacted] cannot ensure the security and compliance of the system's computing environment. System misconfigurations and vulnerabilities could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] to fulfill its mission requirements.

[redacted]:

Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment. Consequently, potential vulnerabilities and control weaknesses may not be identified that could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] to fulfill its mission requirements.

Without remediating critical and medium risk vulnerabilities on a timely basis, DOI cannot ensure the security and compliance of the system's computing environment. System misconfigurations and vulnerabilities could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for DOI to fulfill its mission.

We recommend [redacted]:

15. Remediate [redacted] vulnerabilities associated with [redacted] in accordance with DOI security control standards.

We recommend [redacted]:

16. Implement a process to enforce the performance and documentation of system security patch and update testing and documentation of management approvals prior to the implementation such patches and updates into the [redacted] production environment.

We recommend [redacted]:

17. Improve Configuration Management Plan procedures to require the documentation of testing and impact analyses for security patches and system changes for [redacted].
18. Identify and document appropriate STIG(s) and applicable audit checks for the [redacted] system to evaluate baseline configuration compliance.
19. Configure the [redacted] policy to scan for all applicable audit checks defined in the established STIG(s) for [redacted].
20. Document and maintain policy deviations from the applicable STIG following [redacted]'s STIG Exception Process.
21. Create POA&Ms to document required remediation steps for any untimely remediated failed audit checks identified on the [redacted] system.
22. Require [redacted] management to design and implement a process to retain CM evidence supporting its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Rev 4.

We recommend [redacted]:

23. Update [redacted] patch management policies, procedures, and processes to require that patches are tested and approved prior to implementation and such activities are documented.
24. Document its review of [redacted] scan reports for the [redacted] system, including the justification for vulnerabilities not remediated timely in accordance with defined Department and Bureau timeframes.
25. Remediate [redacted] vulnerabilities in accordance with DOI policy and [redacted] Vulnerability Scanning and Patch Management requirements, and document the justification and mitigating factors for vulnerabilities that cannot be remediated timely.
26. Enhance the Bureau's vulnerability management oversight process to include the [redacted] system in the Vulnerability Management coordination meetings.

We recommend [redacted]:

27. Implement an enforcement process to ensure [redacted] patches are consistently implemented in the time period specified by the DOI Security Control Standards.

We recommend [redacted]:

28. Design and implement a process to ensure CM, risk assessment, and system and information integrity documentation is retained to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53 Rev 4. Security and Privacy Controls for Federal Information System and Organizations.
29. Remediate the [redacted] vulnerability, configure the server to mitigate the vulnerability that could [redacted].
30. Remediate vulnerabilities associated with [redacted] and configure the [redacted] develop a POA&M for vulnerabilities that cannot be remediated timely in accordance with DOI security control standards.

4. Protect Function: Implementation of the IAM Program.

The table below lists deficiencies in the IAM program.

FISMA domain	Summary of Deficiencies
IAM	DOI established an IAM program; however, DOI did not ensure that: • Privileged user access was reviewed and approved for one information system at [redacted]. • Personnel security procedures and related audit artifacts were maintained at [redacted]. • User account management procedures were followed at [redacted]. • A process to enforce completion of DOI required user access agreements, [redacted] forms, and security awareness training prior to provisioning user access was implemented at [redacted]. • Personnel security program and reinvestigation processes were followed at [redacted]. • Periodic reinvestigation of non-privileged users were conducted in accordance with investigation requirements at [redacted]. • A process to perform weekly audit log reviews to monitor privileged user activities was documented and implemented at [redacted]. • User access request forms, [redacted] forms, personnel risk designation documentation, and privacy agreements were maintained at [redacted]. • A system use notification or banner for publicly available information systems was defined and implemented at [redacted].

We performed the following procedures and noted the following deficiencies in 9 of 12 Bureaus' and Offices' IAM programs: [redacted].

[redacted]:

We inquired of [redacted] management and were informed that while management performed an annual review of application user access, a similar review of [redacted] – including those used by [redacted] – was not performed.

Also, we noted audit evidence related to risk designation and investigation for [redacted] users was not available for inspection; therefore, we determined controls related to the personnel security and screening process were ineffective.

[redacted]:

We selected and tested 15 [redacted] non-privileged users to determine whether appropriate screening procedures were followed in accordance with policy. We noted that sufficient audit evidence for four such users was not available. Also, we tested one new [redacted] user to determine whether the user's access request form was appropriately completed prior to configuration of such access. However, [redacted] management was unable to provide evidence demonstrating that the user's access was in fact authorized prior to its configuration in the system.

[redacted]:

We selected and tested two new [redacted] system users that were added to the system since October 2020. We found that one of those users did not complete the required user access agreement, [redacted] form, and security awareness training prior to gaining system access, as is required per DOI Security Control Standards.

[redacted]:

We inspected personnel security risk designation artifacts for two privileged users assigned to the [redacted] system to determine whether the appropriate background checks were performed in accordance with DOI Office of the Secretary Federal Investigative Standards.

Based on procedures performed, we determined that one of those users was last subject to a [redacted] investigation in 2012. However, we noted that a [redacted] investigation is defined as [redacted] and is subject to reinvestigation every [redacted]. Upon notification of the control deficiency, [redacted] management initiated a reinvestigation for the user in question.

[redacted]:

We inspected personnel security risk designation artifacts for a selection of non-privileged [redacted] users to determine whether the appropriate background check was performed.

Based on procedures performed, we noted that reinvestigations of two users selected for testing were not processed timely. Specifically, we noted one user completed a [redacted] investigation in [redacted], and the second user completed a [redacted] investigation in [redacted]. We noted that a [redacted] investigation is defined as a [redacted] and is subject to reinvestigation every [redacted], while [redacted] is defined as a [redacted] and is subject to reinvestigation every [redacted]. Upon notification of the control deficiency, [redacted] management initiated reinvestigations for both users in question.

[redacted]:

We inquired of [redacted] management and were informed that procedures to review and monitor [redacted] for [redacted] activity were not implemented, as is required by DOI Security Control Standards.

[redacted]:

We inquired of [redacted] management and requested audit documentation in support of testing over the IAM FISMA Metric Domain. We noted that management was unable to provide audit documentation in a timely manner for the following: (1) user access agreements for any of the 5 new [redacted] users selected for testing, (2) ROB forms any of the [redacted] users selected for testing, and (3) position risk designation and personnel screening artifacts for the 1 user selected for testing.

[redacted] management continued to collect artifacts after established audit document submission due dates to provide evidence; however, we were unable to review and inspect the artifacts after such dates.

[redacted]:

We inquired of [redacted] management and requested audit documentation in support of testing over the IAM FISMA Metric Domain; however, management was unable to provide audit documentation supporting the performance/completion of position risk designations, user access agreements, ROBs, and privacy agreements for the [redacted] information system in a timely manner.

[redacted] management continued to collect artifacts after established audit document submission due dates; however, we were unable to review and inspect the artifacts after such dates.

[redacted]:

We inquired of [redacted] management to determine whether the publicly available system [redacted] was configured to display a system use notification or warning banner upon logon. We were informed that [redacted] management did not established a system use notification or warning banner to inform users of the authorized use of [redacted] prior to accessing the system, as was required by DOI Security Control Standards.

GAO *Standards for Internal Control in the Federal Government*, states:

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.

3.11 Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

DOI Security Control Standard Access Control, version 4.1 Account Management - AC-2, states:

The organization:

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

DOI Security Control Standard, PS-3 Personnel Screening, states:

The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to Office of Law Enforcement and Security (OLES) Personnel Security and Suitability Program investigation requirements.

DOI Security Control Standard, PS-6 Access Agreements, states:

The organization:
1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements *at least every two years*; and
3. Ensures that individuals requiring access to organizational information and information systems:
   - Sign appropriate access agreements prior to being granted access; and
   - Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or *System Owner-defined frequency*

DOI Security Control Standard Planning (PL), version 4.1, PL-4 Rules of Behavior, states:

The organization:
a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
c. Reviews and updates as needed the rules of behavior at least annually; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

DOI Security Control Standard Awareness and Training (AT), Version 4.1, AT-2 Security Awareness Training, states:

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

a. As part of initial training for new users.
b. When required by information system changes; and
c. Annually thereafter.

DOI OS Federal Investigation Standards

Tier 3 Investigation, Section 8.4.1 Frequency, states: Subjects occupying Tier 3 positions, as defined in paragraph 8.1, shall be reinvestigated such that 100 percent are conducted at least once every five years and as event-driven, subject to implementing guidance.

DOI OS Federal Investigation Standards
Tier 2 Investigation, Section 7.4.1 Frequency, states: Subjects in Tier 2 positions, as defined in paragraph 7.1, shall be reinvestigated at least once every five years and as event-driven, subject to implementing guidance.

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

> The organization:
> a. Reviews and analyzes information systems audit records at least weekly for indications of inappropriate or unusual activity; and
> b. Reports findings to designated organizational officials

NIST SP 800-53, Rev. 4, PL-4 Rules of Behavior, states:

> The organization:
> a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
> b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
> c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and
> d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

NIST SP 800-53, Rev. 4, PS-2 Position Risk Designation, states:

> The organization:
> a. Assigns a risk designation to all organizational positions;
> b. Establishes screening criteria for individuals filling those positions; and
> c. Reviews and updates position risk designations [Assignment: organization-defined frequency].

[redacted]:

[redacted] management informed us that it did not prioritize the establishment of procedural requirements to retain supporting documentation evidencing the performance of [redacted] reviews.

[redacted]:

[redacted] management informed us that it did not prioritize the establishment of procedural requirements to retain documentation evidencing identity and access management processes.

[redacted]:

The [redacted] was out of office when the selected user was granted access to the system. The ISSO's backup was not fully aware of the process used to ensure that new [redacted] users appropriately complete the required user access agreement, ROB form, and security awareness training prior to granting user access to the system.

[redacted]:

[redacted] management was not aware [redacted] personnel reinvestigations were required.

[redacted]:

[redacted] management informed us that it did not prioritize the establishment of procedural requirements to require [redacted] offices to use the [redacted] database to track personnel screening status and start the background reinvestigation process when appropriate.

[redacted]:
We were informed that, due to inadequate staffing and resource prioritization, [redacted] management did not implement a process to periodically review and monitor the [redacted] for [redacted].

[redacted]:
Due to lack of internal communications following change in personnel assignments within [redacted], [redacted] management was unable to provide sufficient audit documentation within the period designated by the auditors.

[redacted]:
Due to lack of internal communications following change in personnel assignments within [redacted], [redacted] management was unable to provide sufficient audit documentation within the period designated by the auditors.

[redacted]:
[redacted] management was unaware of the requirement to implement a system use notification or warning banner on publicly available information systems.

[redacted]:
Not reviewing [redacted] on a periodic basis introduces risk that inappropriate accounts or privileges may not be identified, which could lead to unauthorized access to and modification of information system resources and data.

Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:
Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:
If users are granted access to systems prior to their completion of training, system use agreements and/or ROB forms, the risk is increased that such users may fail to use and manage systems in compliance with security requirements, thereby rendering such systems vulnerable to internal and external threats.

[redacted]:
Failing to perform security reinvestigations timely increases the likelihood that personnel security risk factors go unnoticed, thereby rendering related systems vulnerable to various threat vectors, including those associated with agency insiders.

[redacted]:
Failing to perform security reinvestigations timely increases the likelihood that personnel security risk factors go unnoticed, thereby rendering related systems vulnerable to various threat vectors, including those associated with agency insiders.

[redacted]:
Without the timely identification of unauthorized or inappropriate user activity, there is an increased risk of unauthorized access to and modification of information system resources and data.

[redacted]:
Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:
Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:
System use notifications or warning banners serve as a deterrent to users that are contemplating the performance of unauthorized system activities. The absence of such messaging may leave such users emboldened to carry out unauthorized activities, thereby exposing the system and its data to increased risk of compromise.

We recommend [redacted]:

31. Implement a periodic review of [redacted], as appropriate in accordance with DOI Security Control Standards.
32. Require the retention of personnel security documentation to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

We recommend [redacted]:

33. Require that [redacted] management retain IAM control documentation to support its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

We recommend [redacted]:

34. Enforce completion of DOI required user access agreements, ROB forms, and security awareness training prior to provisioning user access to the [redacted].
35. Update training to inform backup personnel that support the ISSO of their roles and responsibilities when provisioning access to the [redacted].

We recommend [redacted]:

36. Enhance the personnel security program and reinvestigation processes to ensure all [redacted] privileged users are periodically reinvestigated in accordance with DOI Federal Investigative Standards.

We recommend [redacted]:

37. Design and implement a formal policy that requires the regions to utilize the [redacted] to track screening status and start the background reinvestigation process when appropriate.

We recommend [redacted]:

38. Design and implement a process to perform [redacted] of [redacted] in accordance with DOI Security Control Standards.

We recommend [redacted]:

39. Require the retention of user access agreements, ROB forms, and position risk designation and personnel screening documentation for [redacted] users.

We recommend [redacted]:

40. Require the retention of user access agreements, ROB forms, position risk designation and personnel screening documentation, and privacy agreements for [redacted] users.

We recommend [redacted]:

41. Design and implement a system use notification or warning banner for [redacted] users to acknowledge prior to system use.

5. Protect Function: Implementation of the DPP Program.

The table below lists deficiencies in the DPP program.

FISMA Metric Domain	Summary of Deficiencies
DPP	DOI established a DPP program; however, DOI did not ensure that data protection and privacy controls and documentation to support the control environment were implemented and maintained at [redacted].

We performed the following procedures and noted the following deficiencies in 3 of 12 Bureaus' and Offices' DPP programs: [redacted].

[redacted]:

We inquired of [redacted] management and requested audit documentation in support of testing for the DPP FISMA Metric Domain. We were informed that audit documentation demonstrating event monitoring capabilities through tools, such as the [redacted], were not available. Therefore, we were unable to assess whether security tools were in place and operating effectively.

[redacted]:

We inquired of [redacted] management and requested audit documentation in support of testing over the DPP FISMA Metric Domain. However, we were informed that audit documentation was not available for inspection. As a result, the following NIST SP 800-53, revision 4, System and Communication Protection (SC) and SI security controls were determined to be ineffective:

- SC-7 – Boundary Protection,
- SC-18 – Mobile Code,
- SI-3 – Malicious Code Protection, and
- SI-4 – Information System Monitoring.

[redacted]:

We inquired of [redacted] management and requested audit documentation for review and inspection to support testing over the DDP FISMA Metric Domain. However, [redacted] management provided insufficient documentation for inspection. As a result, the following NIST SP 800-53, revision 4, privacy control was determined to be ineffective, AR-5 Privacy Awareness and Training.

[redacted] management continued to collect artifacts after established audit document submission due dates; however, we were unable to review and inspect the artifacts after established audit document submission due dates.

GAO, *Standards for Internal Control in the Federal Government*, states:

> 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.

3.11 – Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

DOI Security Control Standard SI, SI-3 Malicious Code Protection, states:

The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
    1. Perform periodic scans of the information system at a System Owner-defined frequency and real-time scans of files from external sources at one or more; [endpoint; network entry/exit points], as the files are downloaded, opened, or executed in accordance with organizational security policy; and
    2. System Owner selection of one or more: [block malicious code; quarantine malicious code; send alert to administration]. System Owner-defined action in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

DOI Security Control Standard SI, SI-4 Information System Monitoring, states:

The organization:

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

DOI Security Control Standard SC, Version 4.1, SC-7 Boundary Protection, states: The Information System:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.

b. Implements subnetworks for publicly accessible system components that are Selection: physically; logically separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

DOI Security Control Standard SC, Version 4.1, SC-18 Mobile Code, states: The Organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies.
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

NIST SP 800-137, *ISCM for Federal Information System Systems*, Appendix D.1, states:

D.1 Technologies for Data Gathering
Data gathering technologies are those that provide the capability to observe, detect, prevent, or log known security threats and vulnerabilities, and/or remediate or manage various aspects of security controls implemented to address those threats and vulnerabilities. These technologies are primarily implemented at the information systems level (Tier 3). However, they can be configured to support an organization's ongoing security monitoring needs up through mission/business processes and information security governance metrics. Implementing a tool across an organization allows systems within that organization to inherit and leverage said capability. A security automation domain is an information security area that includes a grouping of tools, technologies, and data. Data within the domains is captured, correlated, analyzed, and reported to present the security status of the organization that is represented by the domains monitored. Security automation provides standardized specifications that enable the interoperability and flow of data between these domains. Monitoring capabilities are achieved through the use of a variety of tools and techniques. The granularity of the information collected is determined by the organization, based on its monitoring objectives and the capability of the enterprise architecture to support such activities.

This section describes the tools and technologies within eleven security automation domains that support continuous monitoring:

- Vulnerability Management;
- Patch Management;
- Event Management;
- Incident Management;
- Malware Detection;
- Asset Management;
- Configuration Management;
- Network Management;
- License Management;
- Information Management; and
- Software Assurance.

NIST SP 800-53, Rev. 4, AR-5 Privacy Awareness and Training, states: The Organization:

c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.

[redacted]:

We were informed that [redacted] management did not prioritize the establishment of procedural requirements to retain security tool documentation evidencing the performance of control activities.

[redacted]:

Due to lack of internal communications within [redacted] management was unable to provide sufficient audit documentation to us in a timely manner.

[redacted]:

Due to lack of internal communications following change in personnel assignments within [redacted], [redacted] management was unable to provide sufficient audit documentation to us in a timely manner.

[redacted]:

Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

We recommend DOI:

42. Implement a process to retain data protection and privacy internal control documentation at [redacted] to support its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

6. Detect Function: Implementation of the ISCM Program.

The table below lists deficiencies in the information security continuous monitoring program.

FISMA Metric Domain	Summary of Deficiencies
ISCM	DOI has established an ISCM program; however, DOI did not ensure that: • Results of security control self-assessments conducted weekly were maintained at the [redacted]. • Formal ISCM plans and the assessment of security and privacy controls were documented and implemented in accordance with DOI policy at [redacted]. • ISCM documentation, such as quarterly security control briefing reports provided to the AO for review, were maintained at [redacted].

We performed the following procedures and noted the following weaknesses in 3 of 12 Bureaus' and Offices' ISCM programs: [redacted].

[redacted]:

We inquired of [redacted] management and requested audit documentation, such as results of security control self-assessments for review and inspection to support testing over the ISCM FISMA Metric domain. However, [redacted] management was unable to provide four of five requested self-assessment reports in a timely manner. As a result, we determined the self-assessment process supporting the ISCM program was ineffective.

[redacted] management continued to collect artifacts after established audit document submission due dates; however, we were unable to review and inspect the artifacts after established audit document submission due dates.

[redacted]:

We inquired of [redacted] management and were informed that [redacted] did not complete a comprehensive system control assessment for the [redacted]. Specifically, we noted that most of the security controls had not been independently assessed in the last [redacted]. Therefore, we determined that [redacted] did not develop a formalized security assessment plan in accordance with DOI Security Control Standards to evaluate the effectiveness of the security controls.

We inquired of [redacted] management to determine whether an ISCM plan was documented and implemented and was informed that such a plan was not documented. Furthermore, we determined that although [redacted] management developed an Information Management Technology (IMT) Continuous Diagnostics and Mitigation (CDM) Plan to identify, diagnose, mitigate, and accept risks while continuously monitoring the environment, the CDM Plan did not provide comprehensive monitoring of the environment for security and privacy controls and did not meet the requirements of an ISCM Plan as established by DOI Security Control Standards.

[redacted]:

We inquired of [redacted] management and requested audit documentation, such as security control briefing reports that are provided to the authorizing official for review and inspection, to support testing over the ISCM FISMA Metric Domain. However, [redacted] management was unable to provide the two security control briefing reports that we selected for testing in a timely manner. As a result, we determined associated security controls supporting the ISCM program were ineffective.

[redacted] management continued to collect artifacts after established audit document submission due dates; however, we were unable to review and inspect the artifacts after such dates.

GAO, *Standards for Internal Control in the Federal Government*, states:

> 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.
> 3.11 Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

DOI Security Control Standards SI, SI-4 INFORMATION SYSTEM MONITORING Control, states: The organization:

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

DOI Security Control Standards, Security Assessment and Authorization, version 4.1, CA-2 Security Assessments, states: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:
    1. Security controls and control enhancements under assessment;
    2. Assessment procedures to be used to determine security control effectiveness; and
    3. Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]

DOI Security Control Standards, Security Assessment and Authorization, version 4.1, CA-7 Security Assessments, states:

> The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
> a. Establishment of *System Owner-defined* metrics to be monitored;
> b. Establishment of *System Owner-defined* frequencies for monitoring and *System Owner-defined frequencies* for assessments supporting such monitoring
> c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy
> d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
> e. Correlation and analysis of security-related information generated by assessments and monitoring;
> f. Response actions to address results of the analysis of security-related information; and
> g. Reporting the security status of organization and the information system to the Authorizing Official at least quarterly.

NIST SP 800-137, *ISCM for Federal Information System Systems*, Appendix D.1, states the following:

> D.1 TECHNOLOGIES FOR DATA GATHERING
> Data gathering technologies are those that provide the capability to observe, detect, prevent, or log known security threats and vulnerabilities, and/or remediate or manage various aspects of security controls implemented to address those threats and vulnerabilities. These technologies are primarily implemented at the information systems level (Tier 3). However, they can be configured to support an organization's ongoing security monitoring needs up through mission/business processes and information security governance metrics. Implementing a tool across an organization allows systems within that organization to inherit and leverage said capability. A security automation domain is an information security area that includes a grouping of tools, technologies, and data. Data within the domains is captured, correlated, analyzed, and reported to present the security status of the organization that is represented by the domains monitored. Security automation provides standardized specifications that enable the interoperability and flow of data between these domains. Monitoring capabilities are achieved through the use of a variety of tools and techniques. The granularity of the information collected is determined by the organization, based on its monitoring objectives and the capability of the enterprise architecture to support such activities.

This section describes the tools and technologies within eleven security automation domains that support continuous monitoring:

- Vulnerability Management;

- Patch Management;
- Event Management;
- Incident Management;
- Malware Detection;
- Asset Management;
- Configuration Management;
- Network Management;
- License Management;
- Information Management; and
- Software Assurance.

[redacted]:

Due to lack of internal communications following change in personnel assignments, [redacted] management was unable to provide sufficient audit documentation within the period designated by the auditors.

[redacted]:

[redacted] management stated that they initially planned to conduct security control testing. However, due to competing priorities and availability of resources, management was unable to complete testing during the performance audit period.

[redacted]:

Due to lack of internal communications following change in personnel assignments, [redacted] management was unable to provide sufficient audit documentation within the period designated by the auditors.

[redacted]:

Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:

Management's failure to design, document and implement a functionality ISCM program and, as part of such a program, periodically assess security controls, increases the likelihood that such controls are not designed to be responsive to relevant risks and/or do not operate in an effective manner that is consistent with security requirements. An ineffective security control environment increases the risk of system and data compromise.

[redacted]:

Management's failure to design, document and implement a functional ISCM program and, as part of such a program, periodically assess security controls, increases the likelihood that security controls are not designed to be responsive to relevant risks and/or do not operate in an effective manner that is consistent with security requirements. An ineffective security control environment increases the risk of system and data compromise.

We recommend [redacted] management:

43. Design and implement a process to retain ISCM documentation, such as [redacted] self-assessment reports, to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 4.

We recommend [redacted]:

44. Allocate adequate resources to periodically assess implemented security and privacy controls for the [redacted] in accordance with DOI Security Control Standards.
45. Document and implement a formal ISCM Plan to provide an ongoing situational awareness to support risk-based management decisions in accordance with DOI Security Control Standards.

We recommend [redacted]:

46. Require retention of quarterly security control briefing reports that are submitted to the AO.

7. Respond Function: Implementation of the IR Program.

The table below lists deficiencies in the IR program.

FISMA Domain	Summary of Deficiencies
IR	DOI has established an IR program; however, DOI did not ensure that: • IR program and associated security tool documentation was maintained at [redacted]. • All security incident tickets involving [redacted] were reported to the US-CERT [redacted].

We performed the following procedures and noted the following weaknesses in 2 of 12 Bureaus' and Offices' incident response program: [redacted].

[redacted]:

We inquired of [redacted] management and requested audit documentation in support of testing over the IR FISMA Metric domain. However, management was unable to provide such audit evidence. As a result, the following NIST SP 800-53, Rev 4, IR and SI security controls were determined to be ineffective:

- SI-4 Information System Monitoring
- IR-5 – Incident Monitoring.

[redacted] management provided evidence of the [redacted] capabilities; however, evidence of [redacted] was not provided to demonstrate that security tools were in place to support privacy, continuous monitoring, and IR controls.

[redacted]:

The [redacted] did not consistently implement established processes to ensure that all security incident tickets involving [redacted] were reported to the US-CERT [redacted], as is required by policy.

We randomly selected and inspected 15 of 100 [redacted] related incident tickets. We determined that 1 of 15 incident tickets was reported [redacted] requirement.

GAO, *Standards for Internal Control in the Federal Government*, states:

> 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.

3.11 – Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

DOI Security Control Standard, Version 4.1, SI-4 INFORMATION SYSTEM MONITORING Control, states: The organization:

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

DOI Security Control Standards, version 4.1, IR-5 INCIDENT MONITORING control, states: The organization tracks and documents information system security incidents.

DOI OCIO, *Enterprise Computer Security Incident Response Plan*, version 1.2, dated April 30, 2019, states:

a. All incidents involving PII are breaches that must be reported to the DOI-CIRC Enterprise Incident Portal
b. Therefore, after initial investigation by the bureaus and offices computer security incident response team (BCSIRT), events that meet the National Institute of Standards and Technology (NIST) definition of an incident are required to be reported to DOI-CIRC within one hour of the determination.

NIST SP 800-137, *ISCM for Federal Information System Systems*, Appendix D.1, states:

D.1 TECHNOLOGIES FOR DATA GATHERING
Data gathering technologies are those that provide the capability to observe, detect, prevent, or log known security threats and vulnerabilities, and/or remediate or manage various aspects of security controls implemented to address those threats and vulnerabilities. These technologies are primarily implemented at the information systems level (Tier 3).

However, they can be configured to support an organization's ongoing security monitoring needs up through mission/business processes and information security governance metrics. Implementing a tool across an organization allows systems within that organization to inherit and leverage said capability. A security automation domain is an information security area that includes a grouping of tools, technologies, and data. Data within the domains is captured, correlated, analyzed, and reported to present the security status of the organization that is represented by the domains monitored. Security automation provides standardized specifications that enable the interoperability and flow of data between these domains. Monitoring capabilities are achieved through the use of a variety of tools and techniques. The granularity of the information collected is determined by the organization, based on its monitoring objectives and the capability of the enterprise architecture to support such activities. This section describes the tools and technologies within eleven security automation domains that support continuous monitoring:

- Vulnerability Management;
- Patch Management;
- Event Management;
- Incident Management;
- Malware Detection;
- Asset Management;
- Configuration Management;
- Network Management;
- License Management;
- Information Management; and
- Software Assurance.

NIST SP 800-53, Rev. 4, IR-6 Incident Reporting, states: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in the most current version of NIST Special Publication 800-61 and at https://www.us-cert.gov/incident-notification-guidelines;

US-CERT Federal Incident Notification Guidelines Notification requirement, states:

a. Agencies must report information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised, to the CISA/US-CERT with the required data elements, as well as any other available information, within one hour of being identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department.

[redacted]:

We were informed by [redacted] management that it did not prioritize the retention of audit evidence supporting system monitoring activities.

[redacted]:

We were informed by [redacted] management that the failure to report a [redacted] incident to US-CERT within [redacted] was the result of an oversight (i.e., human error).

[redacted]:

Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:

The failure to timely report incidents involving PII reduces management and associated authorities' ability to identify and remediate factors causing the incident before PII can be fully exploited.

We recommend [redacted]:

47. Design and implement a process to retain incident response internal control documentation to support its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 4.

We recommend [redacted]:

48. Implement an enforcement process to report incident tickets involving [redacted] to US-CERT within the [redacted], as required by the DOI Enterprise Computer Security Incident Response Plan.

8. Recover Function: Implementation of the CP Program.

The table below lists deficiencies in the CP program.

FISMA Metric Domain	Summary of Deficiencies
CP	DOI has established a CP program; however, DOI did not ensure that: • Information system contingency plans (ISCPs) were reviewed and updated to reflect current operations at [redacted]. • Information system backups were performed at [redacted]. • Functional CP tests or exercises for moderate information systems were performed at [redacted]. • Alternate processing and storage sites were established at [redacted]. • Information system backups and business impact analysis are performed at [redacted]. • A contingency plan that supports all workstations within the [redacted] was documented. • A CP and business impact analysis were reviewed and updated in accordance with DOI requirements at [redacted].

We performed the following procedures and noted the following deficiencies in 5 of 12 Bureaus' and Offices' CP programs: [redacted].

[redacted]:

We obtained and inspected the [redacted] contingency plan and noted that while the plan included contingency events for [redacted], it was last reviewed in April 2019 and did not accurately reflect the current [redacted] environment.

Specifically, we noted that alternate processing and storage sites for [redacted] were in [redacted]; however, the contingency plan did not reflect such. Additionally, we determined the procedures to failover to the alternate site or procedures to leverage alternate storage did not reflect the current process for the [redacted] location. .

[redacted]:

We inquired of [redacted] management and requested audit documentation, such as information system backup tool configuration to demonstrate that system backups are conducted. However, we were informed that requested audit evidence was unavailable for inspection; as a result, we determined the information system back control was not effective.

[redacted]:

The FY21 [redacted] contingency plan exercise scheduled for July 28, 2021 was not conducted. Furthermore, we obtained and inspected documentation evidencing performance of the FY20 [redacted] contingency plan test. Based on procedures performed, we noted management tested the contingency plan via a tabletop exercise, rather than a functional exercise or true drill, as is required for [redacted] systems such as the [redacted].

In addition, [redacted] management did not establish an alternate processing or storage site for the [redacted].

[redacted]:

We inquired of [redacted] management and were informed that [redacted] leveraged the [redacted], which was scheduled for completion in August 2021. However, evidence of contingency plan testing and training and subsequent after-action reporting was not available for inspection. Therefore, we determined that the following NIST SP 800-53, Rev 4, contingency planning security controls were ineffective:

- CP-3: Contingency Training
- CP-4: Contingency Plan Testing.

Also, we were informed the [redacted] did not cover all [redacted] assets. Specifically, [redacted] that are part of the [redacted] accreditation boundary were not included in the [redacted].

Also, we inquired of [redacted] management and requested audit documentation in support of testing over the CP FISMA Metric Domain. However, management was unable to provide documentation evidencing the performance of [redacted] server backups in a timely manner. As are result, we determined that the following NIST SP 800-53, Rev 4, contingency planning security control was ineffective: CP-9: Information System Backup.

Finally, [redacted] management was unable to provide evidence supporting the performance of a business impact analysis in a timely manner.

[redacted] management continued to collect artifacts after established audit documentation submission due dates; however, we were unable to review and inspect the artifacts after such dates.

[redacted]:

We inquired of [redacted] management and obtained and inspected the [redacted] contingency plan and Business Impact Analysis (BIA) and determined that both artifacts have not been reviewed and updated since April 2017 and do not accurately reflect the current [redacted] environment.

Also, we were informed that although aspects of the [redacted] contingency plan were exercised during a 'live event' in the FY21, a full test of the contingency plan has not been performed since FY20. Furthermore, [redacted] management did not document steps taken to activate the contingency plan or lessons learned from the live event. As a result, we determined that [redacted] management did not effectively test the [redacted] contingency plan to establish its viability, as well as organizational readiness to execute the plan in a successful manner.

GAO, *Standards for Internal Control in the Federal Government*, states:

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.

3.11 – Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

DOI Security Control Standards, version 4.1, CP-2 Contingency Plan, states: The organization:

a. Develops a contingency plan for the information system that:
    1. Identifies essential missions and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
    5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    6. Is reviewed and approved by designated officials within the organization.
b. Distributes copies of the contingency plan to System Owner-defined key contingency personnel (identified by name and/or by role) and organizational elements;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system at least annually;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to System Owner-defined key contingency personnel (identified by name and/or by role) and organizational elements; and
g. Protects the contingency plan from unauthorized disclosure and modification.

NIST SP 800-53, Rev. 4, CP-3 Contingency Training, states:

The organization:
1. Provides contingency training to information system users consistent with assigned roles and responsibilities:
    a. Within System Owner-defined time period of assuming a contingency role or responsibility;
    b. When required by information system changes; and
At least annually thereafter.

DOI Security Control Standard CP, version 4.1, CP-6 Alternate Storage Site, states: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

DOI Security Control Standard CP, Version 4.1, CP-7 Alternate Processing Site, states: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within timeframes compliant with the Business Impact Analysis for the system, but no later than 90 days when the primary processing capabilities are unavailable.
b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

DOI Security Control Standards CP, CP-9 Information System Backup, states: The organization:

a. Conducts backups of user-level information contained in the information system at least daily incremental and weekly full;
b. Conducts backups of system-level information contained in the information system at least daily incremental and weekly full;
c. Conducts backups of information system documentation including security-related documentation at least daily incremental and weekly full; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, 3.2 Conduct the Business Impact Analysis (BIA), states:

The organization: As the system design evolves and components change, the BIA may need to be conducted again during the Development/Acquisition phase of the Systems Development Life Cycle (SDLC).

[redacted]:

We were informed by [redacted] management that they did not update the [redacted] contingency plan to ensure it accurately reflected the current environment because of competing priorities.

[redacted]:

We were informed by [redacted] management that it did not prioritize the establishment of procedural requirements to retain supporting documentation to evidence the performance of the data backup control activity.

[redacted]:

[redacted] management informed us that they were not fully aware of DIO Security Control Standards requirements associated with the performance of functional contingency plan tests for [redacted] impact systems.

Furthermore, we were informed by [redacted] management that they did not establish an alternate processing and storage site because of competing priorities and the lack of available IT components at alternate processing and storage location.

[redacted]:

Due to lack of internal communications following change in personnel assignments within the [redacted], management was unable to provide sufficient audit documentation within the period designated by the auditors to complete testing of the control environment. [redacted] management was unable to prioritize the development of a contingency plan to address [redacted] workstation assets.

[redacted]:

We were informed that [redacted] had not reviewed and updated the contingency plan and the BIA or conduct a contingency plan exercise due to inadequate staffing and resource prioritization.

[redacted]:

A lack of an updated contingency plan increases the risk that critical information systems and components are not appropriately identified and prioritized to support the organization's mission/business processes in the event the plan is activated.

[redacted]:

Failure to maintain internal control documentation leaves management and other stakeholders without evidence of control performance and hampers efforts to effectively assess the control environment.

[redacted]:

The lack of a functional contingency plan test exercise presents an increased risk of significant disruption in services provided by the [redacted] system, which could result in data loss and the inability to perform mission critical functions.

The lack of an alternate processing and storage site may result in the system being unrecoverable in the event of a disaster or major incident at or near its primary location, which could adversely impact mission critical functions.

[redacted]:

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

Without conducting the BIA, mission functions are not effectively assessed and, as a result, contingency planning is not aligned with real world considerations and requirements.

Without conducting information system backups, mission essential systems and data may be unavailable for restoration and, as a result, key agency operations may be adversely impacted.

Exclusion of [redacted] workstations increases the risk that the contingency plan does not address all aspects of the capabilities necessary for restoration in accordance with requirements and, as a result, mission-essential resources are unavailable in the event of a disaster.

[redacted]:

A lack of an updated contingency plan increases the risk that critical information systems and components are not appropriately identified and prioritized to support the organization's mission/business processes. Additionally, a lack of an updated business impact analysis increases the risks of the critical mission/business processes not being prioritized and recovery objectives not being defined.

A lack of a contingency plan exercise increases the risk that critical mission business/processes are not recovered timely and the organization's preparation to execute the contingency plan. Additionally, a lack of lessons learned increases the risk of weaknesses and corrective actions not being identified to enhance the overall contingency plan process.

We recommend [redacted]:

49. Review, update, and approve the [redacted] contingency plan to reflect the current environment and operations, to include the [redacted], in accordance with DOI security control standards.

We recommend [redacted]:

50. Design and implement a process to retain data backup internal control documentation to support its internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government, NIST SP 800-53, Rev 4.

We recommend [redacted]:

51. Update the control CP-04 implementation statement within the [redacted] SSP to require a functional contingency plan test.
52. Enforce the requirements outlined in the DOI Security Control Standards for contingency planning and ensure that the [redacted] contingency plan testing includes a functional test and results are documented.
53. Establish an alternate storage and processing site for the [redacted].
54. Document a formal risk acceptance in the event an alternate processing site is not obtainable due to the [redacted] system's unique hardware requirements.

We recommend [redacted]:

55. Coordinate with the [redacted] Coordinator to enforce the requirements outlined in the DOI Security Control Standards for Contingency Planning and ensure contingency plan exercises for moderate impact systems include a functional test and results are documented.
56. Conduct a BIA in accordance with the NIST SP 800-34, Rev 1.
57. Perform and maintain evidence of system and user-level backups in accordance with the DOI Security Control Standards.
58. Design and implement a contingency plan to address [redacted] workstations in accordance with DOI Security Control Standards for contingency plan development.

We recommend [redacted]:

59. Review and update the [redacted] contingency plan and BIA in accordance with the DOI Security Control Standards to reflect the current environment.
60. Conduct an annual contingency plan exercise to measure the effectiveness of the contingency plan and document lessons learned to identify corrective actions in accordance with DOI Security Control Standards.

Conclusion

As part of the FISMA performance audit, 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. We identified control deficiencies associated with the areas of RM, SCRM, CM, IAM, DPP, ISCM, IR, and CP.

Based on the FY 2021 IG FISMA Report Metrics guidance and on the CyberScope results, DOI's information security program was assessed as not effective because the majority of the Cybersecurity Function Areas were assessed at Consistently Implemented (Level 3). We assessed DOI's information security program and practices for its information systems as not effective based on the calculation performed in CyberScope.

We made 60 recommendations related to the control deficiencies we identified during the FISMA performance audits. If effectively implemented by management, these remediations should strengthen DOI's information security program. Based on the control deficiencies identified, we offer two additional recommendations to the Department.

The root causes that led to the control deficiencies identified as part of this performance audit may contribute to control deficiencies for other information systems outside of the scope of this audit. The Department should consider and as deemed necessary, apply these recommendations to its entire universe of systems. Furthermore, DOI should implement robust monitoring capabilities to continually assess the cybersecurity state of these systems to include a process to hold Bureaus and Offices that are responsible for the performance of information security controls accountable for consistent and effective execution of said controls, as well the remediation of identified compliance gaps.

In a written response, DOI concurred with our recommendations and provided planned corrective actions that were responsive to the intent of our recommendations (see next section).

The Department of the Interior's Management Response to the Fiscal Year 2021 Draft OIG FISMA Performance Audit Report, 2021-ITA-037.

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

Recommendation 1[redacted]: Ensure that [redacted] management implements procedures enforcing the requirement to review, update, and approve the SSP annually in accordance with DOI security control standards.

> [redacted] *Response:* [redacted] *will implement procedures that ensure the System Security Plan (SSP) is reviewed and approved at least annually and maintained in accordance with the required standards. ([redacted])*
>
> Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 2[redacted]: Enforce established procedures to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

> [redacted] *Response:* [redacted] *will enforce established procedures to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy. ([redacted])*
>
> Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 3[redacted]: Update policy and procedure review requirements to ensure [redacted] cybersecurity policies and procedures are reviewed within the [redacted] interval in accordance with DOI Security Control Standards.

> [redacted] *Program response for recommendation 3:* [redacted]*: 1) Implement a remediation plan to commit resources to update the outdated policy and procedures documents and to ensure reviews and updates happen at least every* [redacted]*. ([redacted] (Up to Date, due for review on 7/20/2022).*
>
> Responsible Official: [redacted]; POC: [redacted] Target Completion Date: [redacted]

Recommendation 4[redacted]: Review and update the eight outdated policy and procedures documents: [redacted]. Further, ensure such documentation is reviewed and updated on a going-forward periodic basis in accordance with DOI Security Control Standards.

[redacted] *Program response for recommendation 4:* [redacted]

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 5.[redacted]: Document, implement, and maintain both a current state and future state [redacted] that follows DOI Security Standards. The [redacted] should consider information security and the resulting risk to [redacted] DOI operations, assets, and individuals.

[redacted] *Program response for recommendation 5:* [redacted] *Security Control to ensure it meets the DOI PM-7 Security Control Standard (due 7/1/2022). 2) Document, implement, and maintain the current state of [redacted]. (due 10/31/2022). 3) Document, implement, and maintain the future state [redacted] that follows DOI Security Standards. (due 12/30/2022).*

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 6.[redacted]: Enhance the established POA&M review process to ensure that all open POA&Ms are regularly and consistently reviewed to ensure that they are updated and remediated per the defined date(s) established within the POA&M.

[redacted] *response for recommendation 6:* [redacted] *to review [redacted] review process document ([redacted] Guidance on POA&M Management Rev1) (due [redacted])*

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 7.[redacted]: Review [redacted] and update the POA&M's attributes accordingly.

[redacted] *response for recommendation 7:* [redacted] *and update the POAM components accordingly based on assessor comments (Completed [redacted])*

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 8.[redacted]: Implement a process to consistently ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

[redacted] *Management Response:* [redacted] *will implement processes which ensure all open POA&Ms are reviewed and updated in accordance with DOI Policy. This will include ensuring all POA&M milestone estimated completion dates are updated as appropriate; and implementing a process which will allow* [redacted] *leadership to review the successful adherence to this requirement.*

Responsible Official: [redacted]; Target Completion Date: [redacted]

Recommendation 9[redacted]: Ensure all mobile devices are operating the minimum approved [redacted] baseline in accordance with DOI policy or obtain a formal policy exception from the DOI Chief Information Security Officer.

[redacted] *Management Response:* [redacted] *to meet the minimum baseline per DOI requirement.* [redacted] *is implementing a process to enable management to ensure* [redacted] *effectively meets this requirement.*

Responsible Official: [redacted]; Target Completion Date: [redacted]

Recommendation 10[redacted]: Design and implement a process to ensure access control documentation is retained to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 4.

[redacted] *Response:* [redacted] *This recommendation tracked as "* [redacted] *" and related to recommendation 39 herein. The* [redacted] *will (1) Develop automated daily report on active users for* [redacted] *from* [redacted] *; (2) Develop* [redacted] *for regular* [redacted] *requests* [redacted] *and* [redacted] *. All of these user access forms are automated electronic forms maintained in* [redacted] *.*

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 11[redacted]: Implement a process to create and periodically update the cybersecurity risk profile in accordance with OMB A-123 requirements.

[redacted] *Response:* [redacted] *Bureau policy and processes will be developed by the end of* [redacted] *and implemented by end of* [redacted] *. (Note: contingent on the* [redacted] *being fully staffed and the* [redacted] *is onboarded.)*

Responsible Official: [redacted] Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 12[redacted]: Implement a process to ensure all POA&Ms are appropriately reviewed and updated in accordance with DOI policy requirements.

[redacted] *Response:* [redacted] *Quarterly AO reviews are currently being implemented and will be fully implemented by end of* [redacted] *. (Note: contingent on the* [redacted] *being fully staffed and the* [redacted] *is onboarded.)*

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 13. : Implement procedures that ensure the is reviewed, updated, and approved at least annually in accordance with DOI security control standards.

Response (2): Process will be developed by the end of and implemented by end of . (.)

Responsible Official: ; Action Owner: ; Target Completion Date:

Recommendation 14. : Enhance the established DOI policies and procedures to include processes over supply chain component authenticity, anti-counterfeit training, and configuration control for component service and repair.

Response. On behalf of the with finding and will continue working to establish policies and procedures for supply chain component authenticity, anti-counterfeit training and configuration control for component service repair.

Responsible Official: ; POC: ; Target Completion Date:

Recommendation 15. : Implement a process to enforce the performance and documentation of system security patch and update testing and documentation of management approvals prior to the implementation such patches and updates into the environment.

Response: will implement a process to enforce the performance and documentation of system security patch and update testing and documentation of management approvals prior to the implementation such patches and updates into the environment ( )

Responsible Official: ; POC: ; Target Completion Date:

Recommendation 16. : Improve Configuration Management Plan procedures to require the documentation of testing and impact analyses for security patches and system changes for .

Response: will review and update Configuration Management procedures to ensure the documentation of testing and impact analyses for security patches and system changes. will monitor corrective actions via .

Responsible Official: ; Target Completion Date: ; Action Owner:

Recommendation 17. : Identify and document appropriate STIG(s) and applicable audit checks for the system to evaluate baseline configuration compliance.

Response: will identify and document baseline configurations and ensure deviations from the applicable STIG(s) are documented following STIG Exception Process. will monitor corrective actions via .

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 18. [redacted]: Configure the [redacted] compliance scanning policy to scan for all applicable audit checks defined in the established STIG(s) for [redacted].

[redacted] *Response:* [redacted] *will ensure that its vulnerability scanning solution is configured to perform configuration monitoring to verify ongoing baseline compliance.* [redacted] *will monitor corrective actions via* [redacted].

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 19. [redacted]: Document and maintain policy deviations from the applicable STIG following [redacted] STIG Exception Process.

[redacted] *Response:* [redacted] *will identify and document baseline configurations and ensure deviations from the applicable STIG(s) are documented following* [redacted] *STIG Exception Process.* [redacted] *will monitor corrective actions via* [redacted].

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 20. [redacted]: Create POA&Ms to document required remediation steps for any untimely remediated failed audit checks identified on the [redacted] system.

[redacted] *Response:* [redacted] *will develop POA&Ms to document remediation actions for weaknesses caused by failed audit checks.* [redacted] *will monitor corrective actions via* [redacted].

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 21. [redacted]: Require [redacted] management to design and implement a process to retain CM evidence supporting its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Rev 4.

[redacted] *Response:* [redacted] *will develop and implement procedures for conducting and retaining vulnerability scanning configurations and results.* [redacted] *will monitor corrective actions via* [redacted]

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 22. [redacted]: Update [redacted] patch management policies, procedures, and processes to require that patches are tested and approved prior to implementation and such activities are documented.

[redacted] *response for recommendation 22:* [redacted]*: Update patch management policies, procedures, and processes to ensure that patches are tested prior to being implemented* [redacted]*. Update patch management policies, procedures, and processes to ensure that patch approvals are adequately documented* [redacted]

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 23. [redacted]: Document its review of [redacted] vulnerability scan reports for the [redacted] system, including the justification for vulnerabilities not remediated timely in accordance with defined Department and Bureau timeframes.

[redacted] response for recommendation 23: [redacted]: Document review of [redacted] vulnerability scan reports for [redacted] including justification for vulnerabilities not remediated within defined Department and Bureau timeframes (4/29/2022).

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: 4/29/2022

Recommendation 24. [redacted]: Remediate [redacted] vulnerabilities in accordance with DOI policy and [redacted] Scanning and Patch Management requirements, and document the justification and mitigating factors for vulnerabilities that cannot be remediated timely.

[redacted] response for recommendation 24: [redacted]: Document remediation of [redacted] in accordance with policy ([redacted]).
Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 25. [redacted]: Enhance the Bureau's vulnerability management oversight process to include the [redacted] in the Vulnerability Management coordination meetings.

[redacted] response for recommendation 25: [redacted]: Include [redacted] vulnerability management oversight process including Vulnerability Management Sync Up Meetings. (2/25/2022)

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 26. [redacted]: Implement an enforcement process to ensure [redacted] security patches are consistently implemented in the time period specified by the DOI Security Control Standards.

[redacted] Response: [redacted] Corrective Action Tasks: The [redacted] a process to perform [redacted] after every update/patch to catch any missing interim patches, in addition to [redacted] scans, and to take action when needed. A process document was created to list the measures and steps taken by [redacted] to ensure that [redacted] patches are not missed and are applied in the timeframe specified in DOI Security Control Standards.

Responsible Official - Headquarters: [redacted]; Responsible Official - Field: [redacted]
Target Date: [redacted]; Completion Date: [redacted]; Percent Complete: [redacted]

Recommendation 27. : Design and implement a process to ensure CM, risk assessment, and system and information integrity documentation is retained to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53 Rev 4. Security and Privacy Controls for Federal Information System and Organizations.

Response: This recommendation tracked as ' will (1) Document Configuration Management process for , to include documentation of ; (2) Document process for maintaining accurate Information System Component Inventory.

Responsible Official: ; Action Owner: ; Target Completion Date:

Recommendation 28. : Remediate medium risk vulnerabilities associated with in accordance with DOI security control standards.

with recommendation 28 and notes that KPMG report said: "We subsequently inquired of management and inspected system records and determined that management remediated the upon notification of this deficiency." (page 24)

Responsible Official: ; POC:
Recommendation Implemented.

Recommendation 29. : Remediate the vulnerability, configure the server to mitigate the vulnerability that could potentially , and/or formally document risk acceptances for one or both of the identified vulnerabilities.

Response: This recommendation tracked as ' will be generated via an server using a). A POA&M will be developed.

Responsible Official: ; Action Owner: ; Target Completion Date:

Recommendation 30. : Remediate vulnerabilities associated with develop a POA&M for vulnerabilities that cannot be remediated timely in accordance with DOI security control standards.

Response: This recommendation tracked as '

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 31.[redacted]: Implement a periodic review of [redacted], as appropriate in accordance with DOI Security Control Standards.

[redacted] Response: [redacted] will implement a periodic review of [redacted], as appropriate in accordance with DOI Security Control Standards. [redacted])

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 32.[redacted]: Require the retention of personnel security documentation to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

[redacted] Response: [redacted] will require the retention of personnel security documentation to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 33.[redacted]: Require that [redacted] management retain [redacted] control documentation to support its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

[redacted] Response: [redacted] will develop and implement procedures to ensure individuals are screened prior to accessing the information system and access agreements are retained. [redacted] will monitor corrective actions via [redacted]

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 34.[redacted]: Enforce completion of DOI required user access agreements, ROB forms, and security awareness training prior to provisioning user access to the [redacted].

[redacted] response for recommendation 35: [redacted]: Update procedures and implement a process to enforce completion of Department-mandated user access agreements, ROB forms, and security awareness training prior to provisioning user access to [redacted]

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 35. : Update training to inform backup personnel that support the ISSO of their roles and responsibilities when provisioning access to the .

response for recommendation 36: : Conduct staff training to ensure that all personnel involved with the onboarding of new personnel are fully aware of their responsibilities when provisioning access to

Responsible Official: ; POC: ; Target Completion Date:

Recommendation 36. : Enhance the personnel security program and reinvestigation processes to ensure all privileged users are periodically reinvestigated in accordance with DOI Federal Investigative Standards.

Response: management will implement a process to ensure all Privileged users maintain requirement for periodic reinvestigation as appropriate. This will include process development and management visibility into successful completion of the required activity.

Responsible Official: ; Technical Official, ; Target Completion Date:

Recommendation 37. : Design and implement a formal policy that requires the regions to utilize the BIM database to track screening status and start the background reinvestigation process when appropriate.

Response: Corrective Action Tasks: An Memo regarding mandatory use of the was sent on 11/03/2021 to

The mandatory use of as outlined in the memo will be incorporated under the Section 5 - Prescreening (Pre-Investigation phase) and under Section 12 - Suitability Actions and Appeals (Post-Adjudication phase) within the currently under development.

Responsible Official – Headquarters: ; Responsible Official - Field: Target Date: ; Completion Date: ; Percent Complete:

Recommendation 38. : Design and implement a process to perform weekly reviews of in accordance with DOI Security Control Standards.

Response: Contract will be issued to implement a capability and associated processes.

Responsible Official: ; Action Owner: ; Target Completion Date:

Recommendation 39. :Require the retention of user access agreements, ROB forms, and position risk designation and personnel screening documentation for .

Response: This recommendation tracked as " " and related to recommendation 10 herein. The will ensure (1) All user access forms ( ) and Rules of Behavior (FISSA Completion Certificate) are maintained electronically in . (2) Position Risk Designation for are inherited controls from the boundary. (3) Ensure that processes are documented and verify.

Responsible Official: ; Action Owner: ; Target Completion Date:

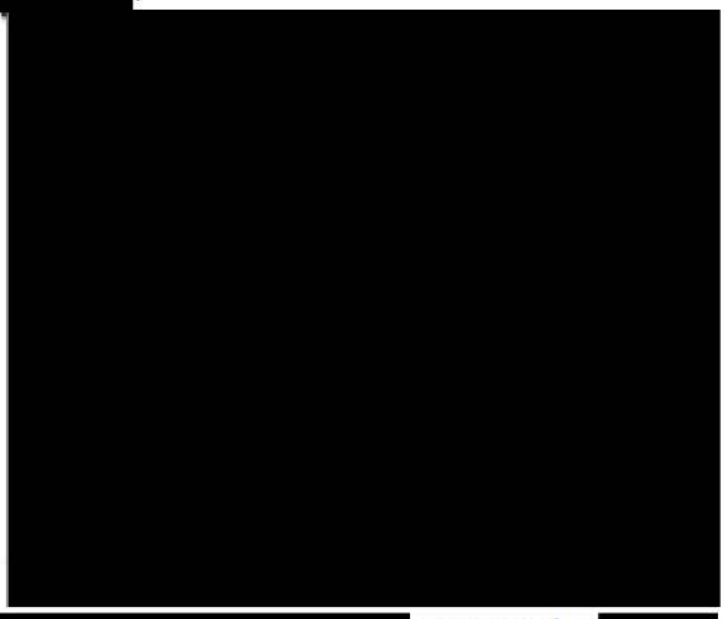
Recommendation 40. : Require the retention of user access agreements, ROB forms, position risk designation and personnel screening documentation, and privacy agreements for users.

Partially with the finding. uses departmental processes including the Rules of Behavior and Privacy Training for privacy agreements for system access. will review the implementation statements to ensure they are accurate and will update audit documentation for .

Responsible Official- ; POC – ; Target Completion Date

Recommendation 41. : Design and implement a system use notification or warning banner for users to acknowledge prior to system use.

Response (42): applied the warning banner for to their system during the next maintenance cycle. The banner was implemented during early .



was opened on to document the Audit finding and document milestones and a resolution that was already completed. will be presented to , for closure on .

Responsible Official: ; Target Completion Date:

Recommendation 42. ; 42. ; 42. : Implement a process to retain data protection and privacy internal control documentation at to support its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST Special Publication 800-53, Rev 4.

Response: will review and update procedures to ensure the of continuous monitoring and incident monitoring. will monitor corrective actions via .

Responsible Official: ; Target Completion Date: ; Action Owner:

response for recommendation 42: : Develop and implement processes and procedures that will ensure documentation and information is available to address audit requirements. ( ). Ensure documents and control artifacts are uploaded to repository. ( ).

Responsible Official: ; POC: ; Target Completion Date:

Partially with the finding. uses departmental processes including completed PIA's and Privacy Training for privacy agreements. will review the implementation statements to ensure they are accurate and will update audit documentation for .

Responsible Official- ; POC – ; Target Completion Date

Recommendation 43. : Design and implement a process to retain , such as self-assessment reports, to support operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 4.

Response: This recommendation tracked as ' Self-Assessment for FY22 is scheduled to be completed by . Quarterly AO Briefing in early .

Responsible Official: ; Action Owner: ; Target Completion Date:

Recommendation 44. : Allocate adequate resources to periodically assess implemented security and privacy controls for the in accordance with DOI Security Control Standards.

Response: is currently working to fully staff the .

Responsible Official: ; Action Owner: ; Target Completion Date:

Recommendation 45[redacted]: Document and implement a formal [redacted] to provide an ongoing situational awareness to support risk-based management decisions in accordance with DOI Security Control Standards.

[redacted] Response: [redacted] Draft concept developed in FY 2021 and some work has been performed in developing standardized Bureau-wide control implementation statements. (Note: contingent on the [redacted])

Responsible Official: [redacted]; Action Owner: [redacted] Target Completion Date: [redacted]

Recommendation 46[redacted]: Require retention of quarterly security control briefing reports that are submitted to the AO.

[redacted] with the audit finding and will retain the quarterly briefings to the AO for [redacted].

Responsible Official- [redacted]; Target Completion Date [redacted]

Recommendation 47[redacted]: Design and implement a process to retain incident response internal control documentation to support its system of internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 4.

[redacted] Response: [redacted] will review and update procedures to ensure the [redacted] results are retained in support of continuous monitoring and incident monitoring. [redacted] will monitor corrective actions via [redacted].

Responsible Official: [redacted]; Target Completion Date: [redacted]; Action Owner: [redacted]

Recommendation 48[redacted]: Implement an enforcement process to report incident tickets involving [redacted] to US-CERT within the [redacted], as required by the [redacted].

[redacted] response: [redacted] has an established SOP and SLA to report incidents involving [redacted] to US-CERT within [redacted] has or will take the following corrective actions:

(1) [redacted] analysts will receive regular training to review US-CERT incident reporting procedures. This will be detailed in a [redacted] policy/manual document
(2) [redacted] will send immediate notification to all [redacted] team members when incidents are reportable to US-CERT. This is implemented via automated notifications configured in [redacted].
(3) [redacted] will develop a process to audit performance of reporting incidents to US-CERT. This process will be documented and reviewed within a [redacted] document.

Responsible Official: [redacted] POC: [redacted]; Target Completion Date: [redacted]

Recommendation 49. : Review, update, and approve the contingency plan to reflect the current environment and operations, to include the , in accordance with DOI security control standards.

Response: will review, update, and approve the contingency plan to reflect the current environment and operations, to include the , in accordance with DOI security control standards.)

Responsible Official: ; POC: ; Target Completion Date:

Recommendation 50. : Design and implement a process to retain data backup internal control documentation to support its internal controls and operational needs as required by the GAO Standards for Internal Control in the Federal Government, NIST SP 800-53, Rev 4.

Response: will develop and implement procedures to ensure that backups are retained and tested for integrity and reliability prior to performing restoration activities. will monitor corrective actions via .

Responsible Official: ; Target Completion Date: ; Action Owner:

Recommendation 51. : Update the control CP-04 implementation statement within the to require a functional contingency plan test.

response for recommendation 51: : Update the control CP-04 implementation statement within the to require a functional contingency plan test ( )

Responsible Official ; POC: ; Target Completion Date:

Recommendation 52. : Enforce the requirements outlined in the DOI Security Control Standards for contingency planning and ensure that the plan testing includes a functional test and results are documented.

response for recommendation 52: : Complete a functional contingency test that meets the requirements outlined in the DOI Security Control Standards for contingency planning and ensure that the plan results are documented.)

Responsible Official: ; POC: ; Target Completion Date:

Recommendation 53. : Establish an alternate storage and processing site for the .

response for recommendation 53: : Establish an alternate storage and processing site for thee or document a formal risk acceptance in the event an alternate processing site is not obtainable due to

[redacted]

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 54. [redacted]: Document a formal risk acceptance in the event an alternate processing site is not obtainable due to the [redacted] requirements.

[redacted] response for recommendation 54: [redacted]: Establish an alternate storage and processing site for the [redacted] or document a formal risk acceptance in the [redacted]

Responsible Official: [redacted]; POC: [redacted]; Target Completion Date: [redacted]

Recommendation 55. [redacted]: Coordinate with the [redacted] to enforce the requirements outlined in the DOI Security Control Standards for Contingency Planning and ensure contingency plan exercises for [redacted] impact systems include a functional test and results are documented.

[redacted] Response: [redacted] This recommendation tracked as "[redacted]". Review [redacted] to validate which [redacted] components may be covered under [redacted]. Develop specific [redacted] Contingency Plan.

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 56. [redacted]: Conduct a business impact analysis (BIA) in accordance with the NIST SP 800-34, Rev 1.

[redacted] Response: [redacted] This recommendation tracked as "[redacted]". Conduct and document [redacted] Business Impact Analysis.

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 57. [redacted]: Perform and maintain evidence of system and user-level backups in accordance with the DOI Security Control Standards.

[redacted] Response: [redacted] This recommendation tracked as "[redacted]". Verify that [redacted] servers (file & print) are included in [redacted] and document accordingly.

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 58. [redacted]: Design and implement a contingency plan to address [redacted] workstations in accordance with DOI Security Control Standards for contingency plan development.

[redacted] Response: [redacted] This recommendation tracked as "[redacted]". POAM drafted for Contingency Plan to address [redacted] workstations IAW with DOI Policy for Contingency Plan development. [redacted] will update the [redacted] system security plan (SSP) to tailor and address residual contingency plan (CP) responsibilities not covered by inherited

controls; and add a CP reference memorandum that will refer to the SSP.

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 59[redacted]: Review and update the [redacted] contingency plan and BIA in accordance with the DOI Security Control Standards to reflect the current environment.

B/O Management Response (2): [redacted] *plan will be updated once the* [redacted] *are onboarded.*

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

Recommendation 60[redacted]: Conduct an annual contingency plan exercise to measure the effectiveness of the contingency plan and document lessons learned to identify corrective actions in accordance with DOI Security Control Standards.

[redacted] *Response:* [redacted] *will implement an annual Bureau-wide IT contingency plan exercise. Implementation contingent on the* [redacted].

Responsible Official: [redacted]; Action Owner: [redacted]; Target Completion Date: [redacted]

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

The following table summarizes the Cybersecurity Functions 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 FY 2021 CyberScope results.

The Identify function area consists of RM and SCRM. The Protect function area consists of CM, IAM, DPP, and ST. The Detect function area consists of ISCM. The Respond function area consists of IR, and the Recover function area consists of CP.

Table: Cybersecurity Function Deficiencies Identified by Organization

Functions	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Identify		X		X		X			X	X		
Protect		X	X	X			X		X	X	X	X
Detect			X						X	X	X	
Respond			X							X		
Recover		X	X	X					X	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]
AICPA	American Institute of Certified Public Accounts
AO	Authorizing Official
AU	Audit and Accountability
BIA	Bureau of Indian Affairs
BIA	Business Impact Assessment
BIM	Background Investigation Management
BLM	Bureau of Land Management
BOEM	Bureau of Ocean Energy Management
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
CA	Security Assessment and Authorization
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CIRC	Computer Incident Response Center
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

Acronym	Definition
CVE	Common Vulnerability and Exposures
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DOI	United States Department of the Interior
DNS	Domain Name Service
DPP	Data Protection and Privacy
[redacted]	[redacted]
[redacted]	[redacted]
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FWS	US Fish and Wildlife Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GSS	General Support System
HR	Human Resource
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication
IA	Information Assurance
IAM	Identity and Access Management
IG	Inspector General
[redacted]	[redacted]
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan

Acronym	Definition
IT	Information Technology
KPMG	KPMG LLP
LAN	Local Area Network
MAC	Mission Assurance Category
MDM	Mobile Device Management
MS	Microsoft
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
[redacted]	[redacted]
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
PD	Position Description
PDR	Position Risk Designation Record
PIA	Privacy Impact Analysis
PII	Personal Identifiable Information
PIV	Personal Identity Verification
PL	Planning
POA&M	Plan of Action and Milestones
PUB	Publication
R2	Release 2
RA	Risk Assessment

Acronym	Definition
RAID	Redundant Array of Independent Disks
RBST	Role Based Security Training
REV	Revision
RFC	Request for Change
RM	Risk Management
ROB	Rules of Behavior
RTO	Recovery Time Objective
SA	System and Services Acquisition
SC	System and Communication Protection
SCRM	Supply Chain Risk Management
SFTP	Secure File Transfer Protocol
SI	System and Information Integrity
SIEM	Security Information and Event Management
SOL	Office of the Solicitor
SP	Special Publication
[redacted]	[redacted]
SSP	System Security Plan
ST	Security and Awareness Training
STIG	Security Technical Implementation Guide
TIMS	Technical Information Management System
[redacted]	[redacted]
US	United States
US-CERT	US Computer Emergency Readiness Team
USB	Universal Serial Bus
USC	United States Code
USGS	United States Geological Survey

Acronym	Definition
[redacted]	[redacted]
[redacted]	[redacted]
WCVF	Weakness Completion Verification Form

Appendix III – Fiscal Year 2020 Recommendation Status

We reviewed prior year findings and recommendations for which corrective actions had been completed. We did not review corrective actions that were in development or not fully implemented. Below is a summary table of the FY20 FISMA report recommendations and their respective status as of October 31, 2021.

Table 1. FY2020 FISMA Report Recommendations and Status as of October 31, 2021.
21 of 33 Recommendations are Open

Recommendation Description	Status
1. [redacted]: 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.	Open. Target completion date: November 30, 2021
2a. [redacted]: Implement a process to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.	Open. Target completion date: February 1, 2022
2b. [redacted]: Implement a process to ensure that all open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.	Open. Target completion date: October 1, 2021
3. [redacted]: Ensure that all contracting officers are aware of the DOI Purchase Card Policy cloud restrictions.	Closed. June 30, 2021
4. [redacted]: 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.	Open. Target completion date: November 30, 2021
5. [redacted]: 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.	Open. Target completion date: November 30, 2021
6. [redacted]: 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.	Open. Target completion date: November 30, 2021
7. [redacted]: Monitor, update, and document [redacted] baseline requirements in accordance with DOI organizational policies and procedures.	Open. Target completion date: November 30, 2021
8. [redacted]: Update the [redacted] with IT Operations to better ensure system-level vulnerabilities are remediated within the timeframes outlined in DOI Risk Assessment Security Control Standard, RA-5.	Open. Target completion date: November 1, 2021
9. [redacted]: 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] system limitations.	Closed. June 28, 2021
10. [redacted]: Ensure that all [redacted] change requests are documented within the [redacted] ticketing system in accordance with [redacted] policy.	Closed. June 28, 2021

Recommendation Description	Status
11. [redacted]: 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.	Closed. June 10, 2021
12. [redacted]: 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.	Closed. August 27, 2021
13. [redacted]: Design and implement a process to perform weekly [redacted] of all [redacted] user activity	Open. Target completion date: November 30, 2021
14. [redacted]: Complete a Weakness Completion Verification Form (WCVF) or obtain a formal risk acceptance noting the [redacted] to generate a [redacted]	Open. Target completion date: November 30, 2021
15 [redacted]: Ensure [redacted] 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.	Open. Target completion date: November 1, 2021
16. [redacted]: Develop and implement a process for the reviews of [redacted] and perform a reconciliation between [redacted] to ensure all activities are completely and accurately captured.	Open. Target completion date: November 1, 2021
17. [redacted]: Design and implement a process to periodically review all [redacted] user access to determine if the access is appropriate.	Open. Target completion date: November 1, 2021
18. [redacted]: 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.	Open. Target completion date: November 1, 2021
19. [redacted]: Implement a process to ensure the appropriate personnel screening of individuals is performed as it relates to job responsibilities, prior to authorizing system access.	Open. Target completion date: November 1, 2021
20. [redacted]: Design and implement procedures to ensure [redacted] activity are reviewed and analyzed, in accordance with DOI policy, to identify and address inappropriate or unusual activity.	Closed. June 30, 2021
21. [redacted]: Enforce current account management policy and procedures that require new [redacted] system access to be authorized prior to being provisioned.	Closed. July 12, 2021
22. [redacted]: Design and implement audit and accountability policies and procedures to ensure [redacted] containing [redacted] activity are reviewed and analyzed for inappropriate or unusual activity in accordance with DOI Security Control Standards.	Open. Target completion date: December 1, 2021
23. [redacted]: 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.	Closed. May 5, 2021
24. [redacted]: Design and implement procedures to ensure [redacted] are reviewed and analyzed on a weekly basis for inappropriate or unusual [redacted] activity and to report findings to the appropriate official.	Open. May 5, 2021

Recommendation Description	Status
25. [redacted]: Design and implement a process to review all [redacted] user accounts at least annually, to determine whether access is valid and appropriate.	Open. Target completion date: October 1, 2021
26. [redacted]: Define, document, and implement a formal process for authorizing and provisioning non-privileged user's access to the [redacted] system.	Closed. August 27, 2021
27. [redacted]: [redacted] 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.	Closed. August 27, 2021
28. [redacted]: Ensure the privacy impact assessment for [redacted] is performed and implement a process to ensure the Privacy Impact Assessment (PIA) is reviewed and updated in accordance with DOI privacy policies.	Open. Target completion date: November 30, 2021
29. [redacted]: 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.	Open. Target completion date: October 1, 2021
30. [redacted]: Ensure [redacted] users' complete role-based security training in accordance with DOI security training policies.	Open. Target completion date: October 1, 2021
31. [redacted]: Update the [redacted] Contingency Plan to include procedures to document the lesson learned process in support of the [redacted] Contingency Plan test exercise.	Closed. June 23, 2021
32. [redacted]: 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.	Closed. May 5, 2021

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

The table below presents the Cybersecurity Functions of Identify, Detect, Protect, Respond, and Recover with the associated NIST SP 800-53 security controls that we considered during the performance audit.

Cybersecurity Identify Function: Risk Management	
NIST SP 800-53, Rev 4: CA-3	System Interconnections
NIST SP 800-53, Rev 4: CA-5	Plan of Action and Milestones
NIST SP 800-53, Rev 4: CA-7	Continuous Monitoring
NIST SP 800-53, Rev 4: CM-8	Information System Component Inventory
NIST SP 800-53, Rev 4: CM-10	Software Usage Restrictions
NIST SP 800-53, Rev 4: RA-1	Risk Assessment Policy and Procedures
NIST SP 800-53, Rev 4: RA-2	Security Categorization
NIST SP 800-53, Rev 4: RA-3	Risk Assessment
NIST SP 800-53, Rev 4: PL-2	System Security Plan
NIST SP 800-53, Rev 4: PL-8	Information Security Architecture
NIST SP 800-53, Rev 4: PM-5	Information System Inventory
NIST SP 800-53, Rev 4: PM-7	Enterprise Architecture
NIST SP 800-53, Rev 4: PM-9	Risk Management Strategy
NIST SP 800-53, Rev 4: PM-11	Mission/Business Process Definition
NIST SP 800-53, Rev 4: SA-3	System Development Life Cycle
NIST SP 800-53, Rev 4: SA-8	Security Engineering Principles
Cybersecurity Identify Function: Supply Chain Risk Management	
NIST SP 800-53, Rev 5: PM-30	Supply Chain Risk Management Strategy
NIST SP 800-53, Rev 5: SR-1	Policy and Procedures
NIST SP 800-53, Rev 5: SA-4	Acquisition Process
NIST SP 800-53, Rev 5: SA-5	System Documentation
NIST SP 800-53, Rev 5: SR-3	Supply Chain Controls and Processes
NIST SP 800-53, Rev 5: SR-5	Acquisition Strategies, Tools, and Methods
NIST SP 800-53, Rev 5: SR-6	Supplier Assessments and Reviews
NIST SP 800-53, Rev 5: SR-11	Component Authenticity
Cybersecurity Protect Function: Configuration Management	
NIST SP 800-53, Rev 4: CM-1	Configuration Management Policy and Procedures
NIST SP 800-53, Rev 4: CM-2	Baseline Configuration
NIST SP 800-53, Rev 4: CM-3	Configuration Change Control
NIST SP 800-53, Rev 4: CM-6	Configuration Settings
NIST SP 800-53, Rev 4: CM-7	Least Functionality
NIST SP 800-53, Rev 4: CM-8	Information System Component Inventory
NIST SP 800-53, Rev 4: CM-9	Configuration Management Plan
NIST SP 800-53, Rev 4: SI-2	Flaw Remediation
Cybersecurity Protect Function: Identity and Access Management	
NIST SP 800-53, Rev 4: AC-1	Access Control Policy and Procedures
NIST SP 800-53, Rev 4: AC-2	Account Management
NIST SP 800-53, Rev 4: AC-8	System Use Notification
NIST SP 800-53, Rev 4: AC-17	Remote Access
NIST SP 800-53, Rev 4: IA-1	Identification and Authentication Policy and Procedures
NIST SP 800-53, Rev 4: SI-4	Information System Monitoring

NIST SP 800-53, Rev 4: PL-4	Rules of Behavior
NIST SP 800-53, Rev 4: PS-1	Personnel Security Policy and Procedures
NIST SP 800-53, Rev 4: PS-2	Position Risk Determination
NIST SP 800-53, Rev 4: PS-3	Personnel Screening
NIST SP 800-53, Rev 4: PS-6	Access Agreements
Cybersecurity Protect Function: Data Protection and Privacy	
NIST SP 800-53, Rev 4: SC-7	Boundary Protection
NIST SP 800-53, Rev 4: SC-8	Transmission Confidentiality and Integrity
NIST SP 800-53, Rev 4: SC-28	Protection of Information at Rest
NIST SP 800-53, Rev 4: MP-3	Media Marking
NIST SP 800-53, Rev 4: MP-6	Media Sanitization
NIST SP 800-53, Rev 4: SI-3	Malicious Code Protection
NIST SP 800-53, Rev 4: SI-4	Information System Monitoring
NIST SP 800-53, Rev 4: SI-7	Software, Firmware, and Information Integrity
Cybersecurity Protect Function: Security Training	
NIST SP 800-53, Rev 4: AT-1	Security Awareness and Training Policy and Procedures
NIST SP 800-53, Rev 4: AT-2	Security Awareness Training
NIST SP 800-53, Rev 4: AT-3	Role-Based Security Training
NIST SP 800-53, Rev 4: AT-4	Security Training Records
Cybersecurity Detect Function: Information System Continuous Monitoring	
NIST SP 800-53, Rev 4: CA-1	Security Assessment and Authorization Policy and Procedures
NIST SP 800-53, Rev 4: CA-2	Security Assessments
NIST SP 800-53, Rev 4: CA-6	Security Authorization
NIST SP 800-53, Rev 4: CA-7	Continuous Monitoring
Cybersecurity Respond Function: Incident Response	
NIST SP 800-53, Rev 4: IR-1	Incident Response Policy and Procedures
NIST SP 800-53, Rev 4: IR-4	Incident Handling
NIST SP 800-53, Rev 4: IR-6	Incident Reporting
Cybersecurity Recover Function: Contingency Planning	
NIST SP 800-53, Rev 4: CP-1	Contingency Planning Policy and Procedures
NIST SP 800-53, Rev 4: CP-2	Contingency Plan
NIST SP 800-53, Rev 4: CP-3	Contingency Pan Training
NIST SP 800-53, Rev 4: CP-4	Contingency Plan Testing
NIST SP 800-53, Rev 4: CP-6	Alternate Storage Site
NIST SP 800-53, Rev 4: CP-7	Alternate Processing Site
NIST SP 800-53, Rev 4: CP-8	Telecommunications Services
NIST SP 800-53, Rev 4: CP-9	Information System Backup
NIST SP 800-53, Rev 4: IR-4	Incident Handling

Appendix V – Responses to the FY 2021 FISMA Reporting Metrics for Inspector General

The appendix describes our responses, to the FY2021 FISMA Reporting Metric questions for the annual independent evaluation of DOI's security program. We made these responses on behalf of the DOI OIG. Within the context of the maturity model, Managed and Measurable (Level 4) is an effective level of security at the FISMA Metric Domain, Cybersecurity Function, and overall information security program level.

In accordance with the FISMA reporting instructions, the ratings assigned for each FISMA Metric Domain is determined by a simple majority, whereby the assessed maturity level most frequently provided in response to 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.

The table below 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 2021 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.

Source: FY2021 FISMA Reporting Metrics

For each FISMA question assessed at maturity Level 1, 2, or 3, we explained in the corresponding "Comment" area why a maturity rating of Level 4: Managed and Measurable 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, according to FISMA reporting instructions, results in an overall determination that DOI's information security program is not effective.

- Identify Function: Risk Management – Consistently Implemented (Level 3)
- Identify Function: Supply Chain Risk Management[8] – Defined (Level 2)
- 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 – Consistently Implemented (Level 3)
- Detect Function: Information System Continuous Monitoring – Managed and Measurable (Level 4)

[8] According to the FY 2021 IG FISMA Reporting Metrics, we assessed the maturity levels of the SCRM metrics, but they were not considered in the overall maturity results used in determining the effectiveness of the Identify Function and the overall information security program.

- Respond Function: Incident Response – Consistently Implemented (Level 3)
- Recover Function: Contingency Planning - Consistently Implemented (Level 3)

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 of Identify, Protect, Detect, Respond, and Recover. The Detect Function and the Identity and Access Management and Information Security Continuous Monitoring FISMA Metric Domains were effective. However, DOI's overall information security program was not effective as we identified deficiencies in four of five Functions: Identify, Protect, Respond, and Recover. Specifically, deficiencies were noted in the associated FISMA Metric Domains of Risk Management, Supply Chain Risk Management,[9] Configuration Management, Data Protection and Privacy, Security Training, Incident Response, and Contingency Planning.

We assessed the Detect Function as Managed and Measurable (Level 4) and the Identify, Protect, Respond and Recover Functions at Consistently Implemented (Level 3). Overall, we assessed DOI's information security program and practices as not effective because the majority of the Cybersecurity Functions were assessed at Consistently Implemented (Level 3).

Below are the CyberScope Reporting Metrics and associated maturity levels.

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 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18)?

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 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.

[redacted] did not ensure mobile devices were subject to monitoring processes defined within the organization's information security continuous monitoring strategy. [redacted] did not have a method to ensure hardware assets connected to the network were authorized.

DOI and its Bureaus and Offices can improve their maturity levels by enforcing the capability to deny mobile device access to DOI networks and resources when security and operating system updates have not been applied.

[9] *Supra* note 13.

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 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?

Maturity Level: Managed and Measurable (Level 4). The organization ensures that the software assets, including mobile applications as appropriate, on the network (and their associated licenses), are covered by an organization-wide software asset management (or mobile device 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 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-12, P-13, S-1 – S-3)?

Maturity Level: Managed and Measurable (Level 4). The organization ensures the risk-based allocation of resources based on system categorization, including for the protection of high value assets, as appropriate, through collaboration and data-driven prioritization.

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-39; NIST SP 800-53 Rev. 4: RA-3, PM-9; NISTIR 8286, CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks R-2, R-3, P-14?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed according to DOI defined time frames and appropriate security controls to mitigate risks identified 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. Further, the organization utilizes a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.

[redacted] did not consistently monitor the effectiveness of risk responses to ensure that risk tolerances were maintained at an appropriate level. Bureaus and Offices did not consistently ensure that information in cybersecurity risk registers was maintained and was used to quantify and aggregate security risks, normalize cybersecurity risk information across the organization, and prioritize operational risk response. [redacted] did not maintain or consistently implement procedures utilizing a cybersecurity risk register to manage risk. [redacted] did not create or maintain a risk profile to manage cybersecurity risks associated with operating and maintaining its information systems.

DOI and its Bureaus and Offices can improve their maturity levels by utilizing the results of their system level risk assessments to perform and maintain a Department-wide cybersecurity and privacy risk assessment. Document results in a cybersecurity risk register and serve as an input into the DOI-wide risk management program.

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) Task P-16; 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.

[redacted] did not appropriately update or review its system security architecture documentation in accordance with policy. [redacted] did not review or update the system security plan for a core information system in accordance with established DOI security policies. [redacted] did not define and develop an information security architecture that describes how that architecture was integrated into and supports the Bureau's [redacted].

DOI and its Bureaus and Offices can improve their maturity levels by ensuring information security architectures are integrated with their system development lifecycles and implement security 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 cyber security risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NISTIR 8286, Section 3.1.1, OMB A-123; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; 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 cybersecurity risk management activities and integrate those activities with enterprise risk management processes, as appropriate. Further, stakeholders involved in cybersecurity risk management are held accountable for carrying out their roles and responsibilities effectively.

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) Task A-6, R-3; OMB M-19-03, CSF v1.1, ID.RA-6)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently utilizes POA&Ms to effectively mitigate security weaknesses. The organization utilizes a prioritized and consistent approach to POA&Ms that considers:

- Security categorizations.
- Specific control deficiencies and their criticality.
- Rationale for accepting certain deficiencies in controls.
- POA&M attributes, in accordance with OMB M-04-14.

[redacted] did not consistently manage their POA&Ms attributes in accordance with established DOI policies and procedures.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative performance measures of the effectiveness of their POA&M activities and by considering the information to make appropriate updates, as needed, to ensure that its risk posture is maintained.

9. To what extent does the organization ensure that information about cyber security risks is communicated in a timely manner to all necessary internal and external stakeholders (OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NISTIR 8286)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently utilizes a cybersecurity risk register, or other comparable mechanism to ensure that information about risks are communicated in a timely and effective manner to appropriate 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.

[redacted] did not consistently implement a process to communicate risks timely to internal stakeholders.

DOI and its Bureaus and Offices can improve their maturity levels by implementing a diagnostic and reporting framework to include dashboards to facilitate a view of cybersecurity risks across the department.

10. To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities 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 cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.

DOI and its Bureaus and Offices can improve their Risk Management programs by implementing automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threats exploiting a vulnerability and the resulting impact to DOI systems and data.

11.1 Please provide the assessed maturity level for the agency's Identify - Risk Management program.
The maturity level for the Risk Management program was assessed at Consistently Implemented (Level 3). Four of 10 risk management metrics were assessed at Managed and Measurable (Level 4). Six of 10 risk management metrics were assessed at Consistently Implemented (Level 3).

11.2 Please provide the assessed maturity level for the agency's Identify Function.
The maturity level for the Identify function was assessed at Consistently Implemented (Level 3).

12. To what extent does the organization utilize supply chain risk management policies and procedures to manage SCRM activities at all organizational tiers (NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-1, NIST CSF v1.1, ID.SC-1, NIST 800-161)?

Maturity Level: Defined (Level 2). The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses: - SCRM risk appetite and tolerance - SCRM strategies or controls - Processes for consistently evaluating and monitoring supply chain risk - Approaches for implementing and communicating the SCRM strategy - Associated roles and responsibilities.

DOI has not fully implemented its SCRM strategy across the Department. DOI can improve its maturity level by fully implementing its strategy across the Department and utilize lessons learned in the implementation to review and update its SCRM strategy.

13. To what extent does the organization utilize a supply chain risk management plan(s) to ensure the integrity, security, resilience, and quality of services, system components, and systems (OMB A-130, NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-2, SR-3; NIST 800-161, section 2.2.4 and Appendix E)?

Maturity Level: Defined (Level 2). The organization has defined and communicated its SCRM policies, procedures, and processes. As appropriate, the policies and procedures are guided by the organization wide SCRM strategy (metric #12). At a minimum, the following areas are addressed - Procedures to facilitate the implementation of the policy and the associated baseline supply chain risk management controls as well as baseline supply chain related controls in other families. - Purpose, scope, SCRM roles and responsibilities, management commitment, and coordination amongst organization entities.

DOI did not implement its SCRM policies and procedures for the SCRM program. DOI can improve its maturity level by implementing departmental policies and procedures for managing supply chain risks for products, systems, and services provided by third parties.

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (NIST SP 800-53 REV. 5: SA-4, SR-3 - 6; NIST SP 800-152; NIST SP 800-37 Rev. 2, Section 2.8; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4)?

Maturity Level: Defined (Level 2). The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined - The identification and prioritization of externally provided systems, system components, and services as well how the organization maintains awareness of its upstream suppliers - Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers. - Tools and techniques to utilize the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. - Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.

DOI has not fully implemented its policies and procedures across the Department. DOI can improve its maturity level by fully implementing procedures for assessing and reviewing the supply chain related risks associated with suppliers or contractors and the system.

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems? (800-53 rev 5 SR-11, 11 (1), and 11(2)

Maturity Level: Ad Hoc (Level 1). The organization has not defined and communicated its component authenticity policies and procedures.

DOI can improve its maturity level by defining and communicating its component authenticity policies and procedures to the Bureaus and Offices.

16.1 Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

The maturity level for the Supply Chain Risk Management (SCRM) program was assessed at Defined (Level 2). Three of four SCRM metrics were assessed at Defined (Level 2). One of four SCRM metrics was assessed at Ad Hoc (Level 1).

16.2 Please provide the assessed maturity level for the agency's Identify Function.

The maturity level for the Identify function was assessed at Consistently Implemented (Level 3).

17. 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 available maturity rating.

18. 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.

Prior to the FISMA performance audit, [redacted] created a POA&M for the lack of formalized configuration management (CM) policies and procedures. DOI and its Bureaus and Offices can improve their CM programs by establishing qualitative and quantitative performance measures on the effectiveness of their configuration management plans and programs.

19. 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 2021 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. Further, the organization utilizes lessons learned in implementation to make improvements to its baseline configuration policies and procedures.

[redacted] did not define and implement baseline configuration policies and procedures for one information system. [redacted] documented the control deficiency and created a POA&M for corrective actions. [redacted] did not effectively review its compliance scanning tool configuration to ensure that required Security Testing Implementation Guide (STIG) audit checks were configured and enabled. Additionally, [redacted] did not remediate failed baseline compliance items within the timeframe requirement in accordance with policy [redacted] did not maintain documented baseline configurations for one information system. Prior to the performance audit, [redacted] created a POA&M identifying the need to document configuration management policies and procedures over one information system.

DOI and its Bureaus and Offices can improve their maturity levels by implementing automated controls to detect unauthorized hardware and software on the DOI network.

20. 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 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Maturity Level: Defined (Level 2). The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.

[redacted] did not consistently use lessons learned in implementation to make improvements to its configuration management policies and procedures. [redacted] documented policies and procedures for establishing and maintaining baseline configurations; however, [redacted] did not develop a baseline for one of its information systems. [redacted] created a POA&M associated with the need to document configuration management policies and procedures for one information system. [redacted] did not consistently perform or maintain baseline configuration compliance scans that identify configuration-based vulnerabilities.

DOI and its Bureaus and Offices can improve their maturity levels by consistently assessing and maintaining secure configuration settings for their information systems and remediating vulnerabilities in accordance with DOI security control standards.

21. 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 2021 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: Defined (Level 2). The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, reporting, and correcting information system flaws, testing software and firmware updates prior to implementation, installing security relevant updates and patches within organizational defined timeframes, and incorporating flaw remediation into the organization's configuration management processes.

[redacted] implemented flaw remediation policies and procedures; however, the Bureaus did not utilize lessons learned in implementation to make improvements to its configuration management policies and procedures. [redacted] did not consistently test and approve security patches prior to implementation. [redacted] did not consistently remediate critical, high, and moderate-risk vulnerabilities timely in accordance with DOI security policies and procedures. [redacted] created a POA&M associated with the need to document configuration management policies and procedures for one information system.

DOI and its Bureaus and Offices can improve their maturity levels by consistently implementing flaw remediation policies and procedures and ensuring that security patches are identified, tested, and installed in accordance with DOI security control standards.

22. 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 M19-26, DHS guidance, and its cloud strategy is ensuring that its TIC implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in the TIC initiative, consistent with OMB M-19-26. The organization monitors and reviews the implemented TIC 3.0 use cases to determine effectiveness and incorporates new/different use cases, as appropriate. This is the highest maturity level available.

23. 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 explicit consideration of security impacts prior to change implementation. The organization utilizes lessons learned in implementation to make improvements to its change control policies and procedures.

[redacted] implemented change control policies and procedures; however, the Bureaus did not utilize lessons learned in implementation to make improvements to its change control policies and procedures. [redacted] did not maintain evidence that system changes were tested prior to deployment into production environment. [redacted] created a POA&M associated with the need to document configuration management policies and procedures for one information system. [redacted] did not consistently implement change control processes and activities for one information system.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative metrics to measure the effectiveness of change control activities and developing defined security responses when baseline configurations are changed in an unauthorized manner.

24. To what degree does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its VDP. In addition, the organization:

- Has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public.
- Ensures that newly launched internet accessible systems and services, and at least 50% of internet-accessible systems, are included in the scope of its VDP.
- Increases the scope of systems covered by its VDP, in accordance with DHS BOD 20-01.

DOI and its Bureaus and Offices can improve their maturity levels with establishing a process for monitoring, analyzing, and reporting on the qualitative and quantitative performance measures used to gauge the effectiveness of their vulnerability disclosure policies and disclosure handling procedures.

25.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

The maturity level for the configuration management program was assessed at Consistently Implemented (Level 3). Four of eight configuration management metrics were assessed at Consistently Implemented (Level 3). Two of eight configuration management metrics were assessed at Defined (Level 2). Two of eight configuration management metrics were assessed at Managed and Measurable (Level 4).

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

The maturity level for the Protect function was assessed at Consistently Implemented (Level 3).

26. 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; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?

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.

27. To what degree does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17, 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 integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. The organization uses automated mechanisms (e.g., machine-based, or user-based enforcement), where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy. Examples of automated mechanisms include network segmentation based on the label/classification of information stored; automatic removal/disabling of temporary/emergency/ inactive accounts; and use of automated tools to inventory and manage accounts and perform segregation of duties/least privilege reviews.

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel 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, OMB M-19-17)?

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.

[redacted] did not ensure that all users selected for audit were appropriately screened prior to gaining system access.

DOI and its Bureaus and Offices can improve their maturity levels by implementing automation to centrally document, track, and share risk designations and screening information with necessary parties.

29. 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 PS-6)?

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

[redacted] did not consistently implemented procedures to ensure user access agreements were maintained. [redacted] did not ensure user access agreements and rules of behavior were completed prior to gaining system access. [redacted] did not define and implement an information system use notification and warning banner for its information system that is publicly available.

DOI and its Bureaus and Offices can improve their maturity levels by using automation to manage and review user access agreements for privileged and non-privileged users.

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157,)?

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

31. 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 [organization-defined entry/exit points], networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

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

32. 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 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; CSIP; DHS ED 19-01; CSF: PR.AC-4)?

Maturity Level: Defined (Level 2). All privileged users, including those who can make changes to DNS records, utilize strong authentication mechanisms to authenticate to applicable organizational systems.

[redacted] did not establish procedures or implement processes to [redacted] in accordance with DOI security policies and procedures. [redacted] defined its audit log procedures; however, procedures were not fully implemented for one information system.

[redacted] were not reviewed by independent system personnel. Specifically, segregation of duties was not enforced for the review of [redacted]. Additionally, the administrators did not retain review documentation to validate that the review took place, inappropriate activity was identified, and inappropriate activity was investigated.

[redacted] did not effectively implement separation of duties responsibilities to ensure privileged user activities were limited and segregated. Prior to the audit, [redacted] self-identified a control deficiency and created a POA&M for corrective actions. [redacted] did not consistently review privileged user accounts annually in accordance with DOI security policies and procedures.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring that processes for managing and reviewing privileged accounts are consistently performed in accordance with DOI security policies and procedures.

33. 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-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2021 CIO FISMA Metrics: 2.10 and 2.11)?

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 nonauthorized devices.

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

The maturity level for the identity and access management program was assessed at Managed and Measurable (Level 4). Five of eight identity and access management metrics were assessed at Managed and Measurable (Level 4). Two of eight identity and access management metrics were assessed at Consistently Implemented (Level 3). One of eight identity and access management metrics were assessed at Defined (Level 2).

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

The maturity level for the Protect function was assessed at Consistently Implemented (Level 3).

35. 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) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b))?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its privacy program by:

- Dedicating appropriate resources to the program.
- Maintaining an inventory of the collection and use of PII.
- Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems.
- Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs).
- Using effective communications channels for disseminating privacy policies and procedures.
- Ensuring that individuals are consistently performing the privacy roles and responsibilities that have been defined across the organization.

[redacted] did not consistently assess privacy controls that protect the collection, use, maintenance, sharing, and disposal of PII.

DOI and its Bureaus and Offices can improve their maturity levels by establishing quantitative and qualitative performance measures on the effectiveness of its privacy activities.

36. 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 2021 CIO FISMA Metrics: 2.8, 2.12; 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.

37. 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 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Maturity Level: Consistently Implemented (Level 3). 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 communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization utilizes email authentication technology and ensures the use of valid encryption certificates for its domains.

[redacted] did not maintain evidence of malware and anti-virus software installed on one information system. Also, [redacted] did not maintain configuration settings evidence for security tools used to monitor and evaluate system vulnerabilities. [redacted] did not maintain evidence of security and privacy controls used for network defenses over its contractor managed information system.

DOI and its Bureaus and Offices can improve their maturity levels with establishing qualitative and quantitative measures on the performance of their data exfiltration processes and enhanced network defenses.

38. 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 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its Data Breach Response Plan. Additionally, the breach response team participates in table-top exercises and uses lessons learned to make improvements to the plan as appropriate. Further, the organization can identify the specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.

DOI and its Bureaus and Offices can improve their maturity levels with establishing qualitative and quantitative performance measures on the effectiveness of their Data Breach Response Plan.

39. 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, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)?

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

DOI and its Bureaus and Offices can improve their maturity levels with measuring their privacy awareness training program by obtaining feedback on the content of the training.

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

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

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

The maturity level for the Protect function was assessed at Consistently Implemented (Level 3).

41. 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: Managed and Measurable (Level 4). 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.

42. To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

Maturity Level: Managed and Measurable (Level 4). The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.

43. 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: Consistently Implemented (Level 3). The organization has consistently implemented its organization-wide security awareness and training strategy and plan.

DOI and its Bureaus and Offices can improve their maturity levels with establishing qualitative and quantitative performance measures on the effectiveness of their security awareness and training strategies and plans.

44. 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 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4)?

Maturity Level: Consistently Implemented (Level 3). The organization ensures that its security awareness policies and procedures are consistently implemented. The organization ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined timeframes] and periodically thereafter and maintains completion records. The organization obtains feedback on its security awareness and training program and uses that information to make improvements.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative performance measures of the effectiveness of their security awareness policies, procedures, and practices.

45. 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 2021 CIO FISMA Metrics: 2.15)?

Maturity Level: Consistently Implemented (Level 3). The organization ensures that its security training policies and procedures are consistently implemented. The organization ensures that individuals with significant security responsibilities complete the organization's defined specialized security training (or comparable training for contractors) [within organizationally defined timeframes] and periodically thereafter. The organization also maintains completion records for specialized training taken by individuals with significant security responsibilities. The organization obtains feedback on its security training program and uses that information to make improvements.

DOI and its Bureaus and Offices can improve their maturity levels with establishing qualitative and quantitative performance measures on the effectiveness of their specialized security training policies, procedures, and practices.

46.1. Please provide the assessed maturity level for the agency's Protect - Security Training program.
The maturity level for the security training program was assessed at Consistently Implemented (Level 3). Three of five security training program metrics were assessed at Consistently Implemented (Level 3). Two of five security training program metrics were assessed at Managed and Measurable (Level 4).

46.2. Please provide the assessed maturity level for the agency's Protect function.
The maturity level for the Protect function was assessed at Consistently Implemented (Level 3).

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

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

47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?

Maturity Level: Consistently Implemented (Level 3). The organization's ISCM policies and strategy are 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 policies and strategy.

[redacted] did not formalize its ISCM policies and procedures, and the Continuous Diagnostic and Mitigation Plan was not reviewed or updated in FY 2021.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative performance measures of the effectiveness of their ISCM policies and 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; NIST 800-37, Rev. 2 Task P-7 and S-5)?

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

49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (OMB A-130, 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) Task S-5; NIST SP 800-18, Rev. 1, 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 authorizations of information systems, including the maintenance of system security plans.

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.

[redacted] did not identify and define the performance measures and requirements used to assess the effectiveness of its ISCM program. [redacted] did not formalized its ISCM policies and procedures, and the Continuous Diagnostic and Mitigation Plan was not reviewed or updated in fiscal year 2021. [redacted] defined ISCM processes for data collection, technology, and analysis; however, management did not consistently implement established processes and capture qualitative and quantitative performance measures on the performance of its ISCM program.

DOI and its Bureaus and Offices can improve their maturity levels by integrating metrics associated with 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 - ISCM domain/function.

The maturity level for the information security continuous monitoring domain was assessed at Managed and Measurable (Level 4). Two of four information security continuous monitoring domain metrics were assessed at Managed and Measurable (Level 4). Two of four information security continuous monitoring domain metrics were assessed at Consistently Implemented (Level 3).

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 Managed and Measurable (Level 4) maturity level, the DOI information security continuous monitoring program is considered effective.

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 – National Preparedness)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its incident response plan. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response plan and making updates as necessary.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative performance measures that have been defined in their incident response plans to monitor and maintain the effectiveness of their overall incident response capabilities.

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; CSF, RS.CO-1, OMB M-20-04; FY 2021 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. This is the highest maturity level available.

54. How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its policies, procedures, and processes for incident detection and analysis. In addition, 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. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary.

[redacted] did not maintain evidence of malware and anti-virus software installed on one information system. Also, [redacted] did not maintain the configuration settings over security tools used to monitor and evaluate system vulnerabilities.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative performance measures that have been defined in their incident response plans to monitor and maintain the effectiveness of their overall incident response capabilities. Also, DOI should implement 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 incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements processes to remediate vulnerabilities that may have been exploited on the target system(s), and recovers system operations. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.

The [redacted] did not consistently report [redacted] security incidents to the US Computer Emergency Readiness Team (US-CERT) in accordance with DOI policy.

DOI and its Bureaus and Offices can improve their maturity levels by establishing qualitative and quantitative performance measures of the effectiveness of their incident handling policies and procedures.

56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)?

Maturity Level: Managed and Measurable (Level 4). Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

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-20-04; PPD-41)?

Maturity Level: Managed and Measurable (Level 4). The organization utilizes Einstein 3 Accelerated, and/or other comparable tools or services, to detect and proactively block cyberattacks 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: Consistently Implemented (Level 3). The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

[redacted] did not maintain evidence of malware and anti-virus software installed on one information system. Also, [redacted] did not maintain configuration settings evidence for security tools used to monitor and evaluate system vulnerabilities.

DOI and its Bureaus and Offices can improve their maturity levels by evaluating the effectiveness of its incident response technologies and updating configuration settings, appropriate.

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

The maturity level for the incident response domain was assessed at Consistently Implemented (Level 3). Four of seven incident response domain metrics were assessed at Consistently Implemented (Level 3). Three of four incident response domain metrics were assessed at Managed and Measurable (Level 4).

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

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

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; 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.

[redacted] defined its roles and responsibilities related to contingency planning. However, the information system contingency plans were not reviewed or updated in accordance with DOI security control standards. [redacted] defined the roles and responsibilities related to contingency planning. However, personnel responsible for information system contingency planning did not ensure that the annual contingency plan test or exercise was completed in accordance with DOI security control standards.

61. 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; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?

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

[redacted] defined its process for conducting information system Business Impact Analyses (BIAs); however, a BIA was not conducted for one information system. [redacted] defined its process for conducting information system BIA; however, the BIA was not reviewed and updated to reflect the current computing environment.

DOI can improve its maturity levels by ensuring results of Bureau, Office, and system level BIAs are integrated with enterprise risk management processes. Also, DOI should review results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.

62. 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 2021 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 plans (as appropriate), and occupant emergency plans.

[redacted] developed an information system contingency plan; however, the contingency plan was not reviewed or updated to ensure accuracy and completeness in accordance with DOI security control standards. [redacted] developed an information system contingency plan; however, the contingency plan did not to support all computing assets within the accreditation boundary.

DOI and its Bureaus and Offices can improve their maturity levels by integrating metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, or incident management to deliver persistent situational awareness across the Department.

63. 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 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?

Maturity Level: Consistently Implemented (Level 3). Information System Contingency Plan (ISCP) 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 and continuity of operations plan.

[redacted] completed a contingency plan tabletop exercise in FY 2021; however, moderate-risk information systems were required to perform a functional test in accordance with DOI security control standards. [redacted] did not consistently test information system contingency plans in FY 2021 as required by DOI security control standards.

DOI and its Bureaus and Offices can improve their maturity levels by implementing automated methods to test contingency plans.

64. 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 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Maturity Level: Defined (Level 2). The organization has defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including use of alternate storage and processing sites and Redundant Array of Independent Disks (RAID), as appropriate. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, environment (e.g., cloud model deployed), maximum downtimes, recovery priorities, and integration with other contingency plans.

[redacted] defined their policies and procedures for information system backup and storage. However, [redacted] did not identify an alternate processing site or alternate storage site. Also, [redacted] did not consistently perform information system backup procedures in accordance with established procedures. [redacted] identified an alternate process site; however, the alternate site was located in close proximity to and as a result, subject to the same risks as, the primary site.

DOI and its Bureaus and Offices can improve their maturity levels by following established policies and procedures for information system backup and storage, including the use of alternate storage and processing sites.

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

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

DOI and its Bureaus and Offices can improve their maturity levels with measuring the effectiveness of recovery activities and results are communicated to relevant stakeholders.

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

The maturity level for the contingency planning domain was assessed at Consistently Implemented (Level 3). Four of six contingency planning domain metrics were assessed at Consistently Implemented (Level 3). One of six contingency planning domain metrics was assessed at Managed and Measurable (Level 4). One of six contingency planning domain metric was assessed at Defined (Level 2).

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

No additional testing was performed beyond the above metrics. Based on the Consistently Implemented (Level 3) maturity level, the DOI contingency planning domain 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