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 2023

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

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

Memorandum

APR 30 2024

To: Darren Ash
Chief Information Officer

From: Kathleen Sedney
Assistant Inspector General for Audits, Inspections, and Evaluations

Subject: Reissuance of *Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2023*
Report No. 2023-ITA-008

This memorandum transmits KPMG LLP's Federal Information Security Modernization Act (FISMA) corrected final audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2023. FISMA (Pub. L. No. 113-283) requires Federal agencies to have an annual independent audit of their information security programs and practices performed to determine the effectiveness of such programs and practices. The agency's Office of Inspector General performs this audit or has the discretion to elect that an independent external auditor perform the audit.

KPMG, an independent public accounting firm, performed DOI's FY 2023 FISMA audit under a contract issued by DOI and monitored by our office. As required by the contract, KPMG asserted that it conducted the audit in accordance with generally accepted government auditing standards to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. KPMG is responsible for the findings and conclusions expressed in the audit report. We do not express an opinion on the report or on KPMG's conclusions regarding DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, dated December 2, 2022. KPMG reviewed information security practices, policies, and procedures at DOI's Office of the Chief Information Officer and the following 11 DOI bureaus and offices:

- Bureau of Indian Affairs
- Bureau of Land Management
- Bureau of Reclamation
- Bureau of Safety and Environmental Enforcement
- U.S. Fish and Wildlife Service
- National Park Service
- Interior Business Center
- 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 audit planning.
- 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, configuration management, identity and access management, data protection and privacy, incident response, and contingency planning. KPMG made 29 recommendations related to these control weaknesses that are intended to strengthen 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 work directly with DOI Audit Liaison Officers and the Office of Financial Management to resolve KPMG's recommendations for this audit. The legislation creating our office 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 aie_reports@doioig.gov.

Attachment

The United States Department of the Interior
Office of Inspector General
Federal Information Security Modernization Act of 2014
Fiscal Year 2023 Performance Audit

December 15, 2023

KPMG LLP
1801 K St. NW
Washington, DC

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

December 15, 2023

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 independent performance audit of the United States (US) Department of the Interior's (DOI) information security program and practices for its information systems. We conducted our performance audit during the period of April 1, 2023, to August 25, 2023, and our results are as of October 4, 2023.

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 control deficiencies and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our control 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 fiscal year (FY) ending September 30, 2023 was to conduct an independent performance audit of the DOI information security program and practices related to the financial and nonfinancial related systems in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).

We made a non-statistical selection of in-scope information systems distributed across 11 Bureaus and Offices. These Bureaus and Offices are the Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), Interior Business Center (IBC), National Park Service (NPS), 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 office and information system results by Cybersecurity Function and FISMA Metric Domain to produce results at the Department level.

We assessed the effectiveness of the Department's information security program and practices and the implementation of the National Institute of Standards and Technology (NIST) 800-53 security controls referenced in the FY 2023 IG FISMA Reporting Metrics. DOI did not fully design and implement the NIST SP 800-53, Rev 5, standards during the performance audit period; therefore, we tested select security controls identified in the NIST SP 800-53, Rev 4, and other controls associated with additional security program areas identified in the FY 2023 Core and Supplemental IG Metrics. We did not identify recommended improvements for the Security Training (ST) and Information Security Continuous Monitoring (ISCM) FISMA Domains. We identified needed improvements in the following FISMA Metric Domains: Risk Management (RM), Supply Chain Risk Management (SCRM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Incident Response (IR), and Contingency Planning (CP).

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: • Audit evidence for software licenses was available for inspection for one system at [redacted]. • Plans of Action and Milestones (POA&Ms) were documented and maintained in accordance with DOI policies for [redacted], and [redacted].
2. Protect (CM, IAM, DPP, and ST)	DOI established CM, IAM, and DPP programs; however, DOI did not ensure that: • Privileged user activity was logged and reviewed for the selected systems at [redacted], and [redacted]. • Separation of Duties (SOD) controls were implemented for privileged users for one system at [redacted]. • Critical- and high-risk vulnerabilities were remediated within the DOI required timeframe for selected systems at [redacted], and [redacted]. • Baseline security configurations were monitored and reviewed for compliance for selected systems at [redacted] and [redacted]. • Privileged user access was reviewed at least annually for one system at [redacted]. • Audit evidence for one system at [redacted] was available for inspection to include: o Data in Transit (DIT) encryption; o Patch management documentation; o New user access documentation (e.g., access request forms, acceptable use agreements, rules of behavior (ROB), and risk designation); and o Recertification for privileged users. DOI established a ST program, and we did not identify and report any deficiencies.
3. Detect (ISCM)	DOI has established an ISCM program, and we did not identify and report any deficiencies.
4. Respond (IR)	DOI established an IR program; however, DOI did not ensure that: • Incident tickets involving Personally Identifiable Information (PII) were reported to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery. • The Event Logging (EL) and retention program was operating at the EL-1 maturity tier by August 27, 2022, and the EL-2 maturity tier by February 27, 2023, for the Department.
5. Recover (CP)	DOI established a CP program; however, DOI did not ensure that: • Audit evidence for a formalized information system contingency plan was available for inspection for one system at [redacted].

Based on the maturity levels calculated in CyberScope,[1] we determined DOI's information security program was not effective as it was not consistent with applicable FISMA requirements, Office of Management and Budget (OMB) policy and guidance, and NIST standards and guidelines. According to OMB's *FY23-2024* IG *FISMA Reporting Metrics,* a security program is considered effective if the calculated average of the FY 2023 IG FISMA Reporting Metrics is at least Managed and Measurable (Level 4). Using the OMB's guidance and the CyberScope results, we determined the calculated average of the Cybersecurity Functions were assessed as Consistently Implemented (Level 3).

We made 29 recommendations related to control deficiencies identified during our performance audit that, if effectively implemented by DOI, should strengthen DOI's information security program.

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 its information systems to include a process to hold Bureaus and Offices accountable for identified control deficiencies.

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 2022 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 2023 IG FISMA Reporting Metrics.

We were not engaged to, and did not, render an opinion on the U.S. DOI'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

[1] CyberScope, operated by DHS on behalf of the OMB, is a web-based application designed to streamline information technology (IT) security reporting for federal agencies. It gathers and standardizes data from federal agencies to support FISMA compliance. In addition, IGs provide an independent assessment of effectiveness of an agency's information security program. IGs must also report their results to DHS and OMB annually through CyberScope.

Table of Contents

Background

Mission of the DOI and its Bureaus/Offices

The U.S. 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 OS, the Assistant Secretary for Policy, Management and Budget, Solicitor's Office and Office of Inspector General (OIG). Of those, the following 11 Bureaus and Offices are included within the scope of the OIG FISMA performance audit for FY 2023:

1 The **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 (US) for American Indian, Indian tribes, and Alaska Natives.

2 The **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 **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 **BSEE** is responsible for overseeing the safe and environmentally responsible development of energy and mineral resources on the Outer Continental Shelf.

5 The **FWS** was created to conserve, protect, and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people.

6 The **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.

7 The **OS** is primarily responsible for providing quality services and efficient solutions to meet DOI business needs.

8 The **IBC** is a federal shared service provider that offers Acquisition, Financial Management and Human Resources (HR) systems and services to federal organizations.

9 The **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.

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

11 The **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.

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 (IA) 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 IA 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 IMT 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 2023 IG FISMA Reporting Metrics were aligned with the five function areas in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IG with guidance for assessing the maturity of controls to address those risks.

For FY 2023, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, the Department of Homeland Security (DHS), and the Federal Chief Information Officers and CISOs' councils developed the FY 2023 IG FISMA Reporting Metrics[2] around five Cybersecurity Functions outlined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The FY 2023 IG FISMA Reporting Metrics consisted of 20 Core Metrics and 20 Supplemental Group 1 Metrics organized around the five Cybersecurity Functions.

[2] OMB's *FY 2023-FY2024 IG FISMA Reporting Metrics*

The FY 2023 Core and Supplemental IG FISMA Reporting Metrics were chosen based on alignment with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity,* as well as OMB guidance provided to agencies to further the modernization of federal cybersecurity. OMB provided the following guidance: *Moving the United States (U.S.) Government Toward Zero Trust Cybersecurity Principles (M-22-09), Multifactor Authentication (MFA) and Encryption (EO 14028), Improving the Federal Governments' Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31), Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01), Software Supply Chain Security & Critical Software (Section 4 of EO 14028)* and *FY 2023 Guidance on Federal Information Security and Privacy Management Requirements (M-23-03).*

The FY 2023 Core and Supplemental IG FISMA Reporting Metrics use the CIGIE maturity models for the nine FISMA Metric Domains. **Table 1** below outlines the alignment of the Cybersecurity Framework Functions to the FISMA Metric Domains.

Table 1: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FISMA Metric Domains within the FY 2023 Core and Supplemental IG FISMA Reporting Metrics

Cybersecurity Functions	FISMA Metric Domains
Identity	RM SCRM
Protect	CM IAM DPP ST
Detect	ISCM
Respond	IR
Recover	CP

IG FISMA Scoring

The assessed maturity levels for the nine FISMA Metric Domains (RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by the calculated average. The assessed maturity levels for each FISMA function were determined by the calculated average of its domains.

The maturity model has five levels: Level 1: Ad-hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Framework Function. A security program is considered effective if the calculated average of the FY 2023 Core and Supplemental IG FISMA Reporting Metrics was at least Level 4: Managed and Measurable.

Table 2: IG Assessed Maturity Levels

Maturity Level	Description
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.

The purpose of assessing maturity levels for each metric is to drive continued improvements in cybersecurity maturity across the federal environment and specific agency efforts.

Objective, Scope, and Methodology

The audit objective of our work for the year ending September 30, 2023, 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. We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the 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 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 FY 2023 IG FISMA Reporting Metrics; and
- An inspection of the information security practices, policies, and procedures in use across the following 11 Bureaus and Offices identified by the DOI OIG: BIA, BLM, BOR, BSEE, FWS, IBC, NPS, 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 in consideration of applicable Federal laws and criteria to determine whether the Department and Bureaus policies, procedures and practices were generally consistent with FISMA.

Step B: System level compliance – During this step, we assessed the effectiveness of the Department's information security program and practices and the implementation of the NIST 800-53 security controls referenced in the FY 2023 IG FISMA Reporting Metrics. DOI did not fully design and implement all control requirements outlined the NIST SP 800-53, Rev 5, standards during the performance audit period; therefore, we tested select security controls identified in the NIST SP 800-53, Rev 4, and additional security program areas identified in the FY 2023 Core and Supplemental IG Metrics. During this step, we assessed the implementation of a selection of security controls from the NIST SP 800-53, Rev 4 and 5, for a selection of DOI's information systems.[3]

[3] The OIG judgmentally selected [redacted] unclassified operational systems recorded in the Departments official repository, [redacted], [redacted]). The representative subset included Major Applications, General Support Systems (GSS), Contractor Systems, and Cloud-Based systems with Federal Information Processing Standard (FIPS) 199 security categorizations of "Moderate" and "High." The FIPS 199 ratings are defined by the DOI system owner and authorizing official.

Table 3 documents the information systems audited.

Table 3. DOI Information Systems Audited

	Bureau/Office	Information Systems	[redacted] ID	FIPS 199 Category
1	BIA	[redacted]	[redacted]	[redacted]
2	BLM	[redacted]	[redacted]	[redacted]
3	BOR	[redacted]	[redacted]	[redacted]
4	BSEE	[redacted]	[redacted]	[redacted]
5	FWS	[redacted]	[redacted]	[redacted]
6	IBC	[redacted]	[redacted]	[redacted]
7	NPS	[redacted]	[redacted]	[redacted]
8	OS	[redacted]	[redacted]	[redacted]
9	OSMRE	[redacted]	[redacted]	[redacted]
10	SOL	[redacted]	[redacted]	[redacted]
11	USGS	[redacted]	[redacted]	[redacted]

Results of Review

Based on the maturity levels calculated in CyberScope, we determined DOI's information security program was not effective for all five Cybersecurity Functions and all nine FISMA Metric Domains as it was not consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. A security program is considered effective if the calculated average of the FY 2023 IG FISMA Reporting Metrics is at least Level 4: Managed and Measurable. **Table 4** below depicts the maturity levels for the five Cybersecurity Functions.

Table 4: Maturity Levels for Cybersecurity Functions

Cybersecurity Functions	Assessed Maturity Levels
Identify – RM & SCRM	Defined (Level 2)
Protect – CM, IAM, DPP, and ST	Consistently Implemented (Level 3)
Detect – ISCM	Consistently Implemented (Level 3)
Respond – IR	Consistently Implemented (Level 3)
Recover – CP	Consistently Implemented (Level 3)

Refer to Appendix V, *Responses to the FY 2023 IG FISMA Reporting Metrics*, for the assessed maturity levels for each FY 2023 IG FISMA Metric question.

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 RM and SCRM programs; however, DOI did not ensure that: • Audit evidence for software asset inventory was available for inspection for one system at [redacted] • POA&Ms were documented and maintained in accordance with DOI policies for [redacted], and [redacted].

We performed the following procedures and noted the following deficiencies in the RM programs of the following Bureaus and Offices: [redacted], and [redacted].

[redacted]:

Software asset audit evidence was not available for inspection to evaluate the design, implementation, and operating effectiveness for the NIST SP 800-53 Rev 5, Information System Component Inventory (CM-8) security control for the [redacted] system. As a result, this security control was determined to be ineffective.

[redacted]

Five open bureau-wide [redacted] POA&Ms were selected for inspection, and two of five did not include milestones, which did not adhere to the *DOI OCIO POA&M Coordinator Standard Operating Procedure (SOP)*. Also, three of five selected POA&Ms did not include updated milestones or scheduled completion dates. We informed [redacted] management of the control deficiency, and [redacted] management took immediate action and updated the POA&Ms.

[redacted]

We inspected 15 open [redacted] POA&Ms selected for testing and determined that none of them were documented in accordance with DOI policies. Specifically, we noted that milestones or milestones with scheduled completion dates were not documented.

[redacted]

We inspected five open [redacted] POA&Ms selected for testing determined that two of them were not documented in accordance with DOI policies. Specifically, we noted milestones were not documented.

[redacted]

We inspected 15 open [redacted] POA&Ms selected for testing and determined 9 of them were not documented in accordance with DOI policies. Specifically, we noted the milestones were not documented and/or scheduled completion dates were expired.

Government Accountability Office (GAO), Standards for Internal Control in the Federal Government, dated September 2014, states*:*

> Documentation of the 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.
> 10.03 Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

DOI Security Control Standard (SCS), CM, version 1.0, dated December 2022, CM-8 Information System Component Inventory, states:

> The organization:
> a. Develop and document an inventory of system components that:
> 1. Accurately reflects the system;
> 2. Includes all components within the system;
> 3. Does not include duplicate accounting of components or components assigned to any other system.
> 4. Is at the level of granularity deemed necessary for tracking and reporting; and
> 5. Includes the following information to achieve system component accountability: as defined by the system owner (SO) in the System Security Plan (SSP) hardware inventory list.
> b. Review and update the system component inventory annually at a minimum when new assets/components are added or as defined by the SO in the Configuration Management Plan (CMP).

DOI SCS, Security Assessment and Authorization (CA), version 1, CA-5 POA&M, states*:*

> The organization:
> a. Develop a POA&Ms for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Update existing POA&Ms at least quarterly based on the findings from control assessments, independent audits or Reviews, and continuous monitoring activities.

DOI OCIO POA&M Coordinator SOP, version 7.0, dated February 2023, states*:*

> The organization:
> a. For Severity Code, use the pull down. IV=Low, III=Medium, II=High, I=Critical
> b. Milestones should reflect work done to remediate the finding.
> c. All milestones have been fully populated, including dates of completion.

[redacted]

Due to lack of internal communications within [redacted] and [redacted] management, [redacted] and [redacted] management were unable to provide sufficient audit documentation within the period designated by KPMG.

[redacted], and [redacted]*:*

[redacted], and [redacted] management did not prioritize adherence to the DOI OCIO POA&M Coordinator SOP for the maintenance of POA&Ms to ensure that required fields were appropriately documented within the [redacted] tool.

[redacted]

Without documentation evidencing essential internal control activities, management may not identify control gaps in its processes and procedures. Consequently, potential vulnerabilities and control deficiencies may not be identified and thus could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] and [redacted] management to fulfill its mission requirements.

[redacted], and [redacted]

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

We recommend [redacted]

1. Ensure [redacted] management develop and implement processes and procedures that will ensure documentation and information related to the System Component Inventory (CM-8) control are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5, *Security and Privacy Controls for Information System and Organizations*.

We recommend [redacted], and [redacted]

2. Enhance the POA&M maintenance process to ensure that all bureau-level open POA&Ms are reviewed and updated quarterly in accordance with DOI policy.
3. Ensure all required fields, such as milestone and scheduled completion dates, are documented and defined for each open POA&M.

2. 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: • Critical- and high-risk vulnerabilities were remediated within the DOI required timeframe for the selected systems at [redacted], and [redacted] • Baseline security configurations were monitored and reviewed for compliance for the selected system at [redacted], and [redacted] • Audit evidence for patch management was available for inspection for one system at [redacted]

We performed the following procedures and noted the following deficiencies in the CM Programs of the following Bureaus and Offices: [redacted], and [redacted]

[redacted]

[redacted] management did not consistently implement the process to remediate a high-risk vulnerabilities in accordance with the DOI SCS. Specifically, we inspected 5 of 27 [redacted] vulnerability scan reports for the period of October 2022 through March 2023 for the [redacted] information system and determined one high-risk vulnerability, [redacted], was not remediated within 30 days on five [redacted] servers. On February 14, 2023, the Department classified the vulnerability as a high-risk item; however, as of May 8, 2023, the vulnerability was not remediated. Also, [redacted] management did not create a POA&M to track remediation efforts for the open vulnerability on the [redacted] servers.

[redacted]

[redacted] management did not fully document and implement a process to review the [redacted] and [redacted] server baseline security configurations.

Audit evidence was not available for inspection to determine whether the NIST SP 800-53, Rev. 5, Flaw Remediation (SI-2) security control was designed and implemented for the [redacted] system. As a result, the security control was determined to be ineffective.

[redacted]

[redacted] management did not document policies or procedures and implement a process to generate and review baseline configuration compliance reports for the [redacted] system. We informed [redacted] management of the control deficiency, and [redacted] management took corrective actions to implement a process to review the [redacted] baseline configuration.

We inspected [redacted] scan reports over the [redacted] to determine whether flaw remediation practices were effective and whether critical- and high-risk vulnerabilities were present. Twelve vulnerabilities (four critical- and eight high-risk) were not remediated timely in accordance with the DOI SCS. Specifically, **Table 5** below identifies critical- and high-risk vulnerabilities not remediated timely.

Table 5. Critical- and High-Risk Vulnerabilities Not Remediated Timely.

Security Center Plugin	Plugin Name	Risk Level	Number of Days the Vulnerability Existed Beyond the 30-Day Remediation Period
1. [redacted]	[redacted]	Critical	18+
2. [redacted]	[redacted]	Critical	49+
3. [redacted]	[redacted]	Critical	49+
4. [redacted]	[redacted]	Critical	18+
5. [redacted]	[redacted]	High	18+
6. [redacted]	[redacted]	High	18+
7. [redacted]	[redacted]	High	18+
8. [redacted]	[redacted]	High	18+
9. [redacted]	[redacted]	High	18+
10. [redacted]	[redacted]	High	18+
11. [redacted]	[redacted]	High	18+
12. [redacted]	[redacted]	High	49+

[redacted]

[redacted] management did not design and implement a process to monitor the system baseline security configuration for compliance in accordance with the DOI SCS.

We performed authenticated vulnerability security scans over the [redacted] system to determine whether system patch and CM practices were effective and whether critical-, high-, or medium-risk vulnerabilities were present. Ten vulnerabilities (six critical- and four high-risk vulnerabilities) were not remediated timely in accordance with the DOI SCS. **Table 6** below lists the critical- and high-risk vulnerabilities that were identified.

Table 6. Critical- and High-Risk Vulnerabilities Not Remediated Timely.

Vulnerability Name	Risk Level	Number of Days the Vulnerability Existed Beyond the 30-Day Remediation Period
1. [redacted].	Critical	321
2. [redacted].	Critical	237
3. [redacted]	Critical	125
4. [redacted]	Critical	216
5. [redacted].	Critical	47
6. [redacted]	Critical	20
7. [redacted].	High	68
8. [redacted].	High	68
9. [redacted]	High	96
10. [redacted]	High	34

We informed [redacted] management of the vulnerabilities identified, and management took immediate corrective actions. We inspected reports and confirmed all reported vulnerabilities were remediated.

[redacted]

We performed authenticated vulnerability security scans over the [redacted] system to determine whether system patch and CM practices were effective and whether critical, high, and medium-risk vulnerabilities were present. Eight vulnerabilities (one critical-, four high-, and three medium-risk vulnerabilities) were not remediated timely in accordance with the DOI SCS. Please see **Table 7** below for the list of the critical- and high-risk vulnerabilities that were identified.

Table 7. Critical- and High-Risk Vulnerabilities Not Remediated Timely.

Vulnerability Name	Risk Level	Number of Days the Vulnerability Existed Beyond the 30-Day Remediation Period	Vulnerability Remediated (Yes/No)
1. [redacted].	Critical	86 days	No
2. [redacted]	High	506 days	No
3. [redacted]	High	37 days	Yes
4. [redacted]	High	370 days	Yes
5. [redacted]	High	307 days	Yes
6. [redacted]	Medium	446 days	No
7. [redacted]	Medium	40 days	Yes
8. [redacted]	Medium	446 days	No

We informed [redacted] management of the vulnerabilities, and management took immediate corrective actions. We inspected reports and confirmed four vulnerabilities were remediated. [redacted] management planned to develop POA&Ms to address the four remaining vulnerabilities.

[redacted], Control SI-2 Flaw Remediation*:*

The established CM process must contain the following functions with respect to flaw remediation:

a. Identify software affected by recently announced software flaws and the potential vulnerabilities resulting from those flaws.
b. Incorporating flaw remediation into the established CM process as an emergency change.
c. Testing every patch, service pack, and hot fix for effectiveness and potential side effects on [redacted] information systems before installation.
d. Immediately release security relevant patches, service packs, and hot fixes after testing to all State/Center Office points of contact.
e. Flaws discovered during security assessments, continuous monitoring, or IR activities will be added to the POA&M.

DOI Security Control Standard (SCS) CM, Version 4.1, CM-2(1) Baseline Configuration, states*:*
Control Enhancements: Baseline Configuration | Reviews and Updates

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

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

DOI SCS CM, Version 4.1, CM-6 Configuration Settings, states*:*

The organization:

a. Establishes and documents configuration settings for IT products employed within the information system using US Government Configuration Baseline, or other appropriate checklists from the National Vulnerability Database maintained by the NIST that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

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

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

DOI SCS, System and Information Integrity (SI), version 1.0, dated December 2022, SI-2 Flaw Remediation, 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 DOI-defined time period of the release of the updates; and

d. Incorporates flaw remediation into the organizational CM process.

DOI SCS RA v4.2, RA-5 Vulnerability Scanning Control, states:

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:
    a. Enumerating platforms, software flaws, and improper configurations;
    b. Formatting checklists and test procedures; and
    c. Measuring vulnerability impact.
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities to Internet-accessible systems within fifteen days for critical vulnerabilities, thirty days for critical vulnerabilities on non-Internet accessible systems, thirty days for high-risk/important vulnerabilities on all systems, and within ninety days 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 Continuous Diagnostics and Mitigation (CDM) program and EVSS personnel to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

GAO, Standards for Internal Control in the Federal Government, dated September 2014, 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.

10.03 Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

[redacted]

Due to a lack of oversight and complications with the transition to the [redacted], [redacted] management inadvertently tracked the remediation of the vulnerability through the DOI-CERT ticketing system instead of also creating a POA&M and appropriately tracking the plan and progress through remediation.

[redacted]

[redacted] management did not identity or evaluate the risk associated with the lack of policies and procedures for the review of [redacted] and [redacted] servers baseline configuration and compliance.

Due to lack of internal communications within [redacted] and [redacted] management, [redacted] and [redacted] management were unable to provide sufficient audit documentation within the period designated by KPMG.

[redacted]

[redacted] management did not identify or evaluate the risk associated with not performing reviews over Baseline Configuration Compliance Reports.

[redacted] management did not prioritize adherence to the DOI SCS associated with the performance of vulnerability remediation efforts in response to previous vulnerability scans conducted or create a POA&M for vulnerabilities that could not be remediated timely.

[redacted]

[redacted] management incorrectly relied on the [redacted] change management process to ensure that baseline security configuration changes are maintained. Therefore, [redacted] management did not monitor the [redacted] system security baseline configuration for compliance.

[redacted] management did not identify or evaluate the risk associated with not performing reviews over vulnerability scan results and remediating vulnerabilities in accordance with the DOI SCS.

[redacted]

Due to the emphasis on implementing multi-factor authentication at [redacted] [redacted] management did not prioritize adherence to the DOI SCS associated with the performance of security patch and configuration remediation efforts in response to previous vulnerability scans conducted or create a POA&M for vulnerabilities that could not be remediated timely.

[redacted]

Without remediating and tracking critical-, high-, and medium-risk vulnerabilities on a timely basis, the [redacted] system may be exposed to vulnerabilities.

[redacted]

Without a process to monitor compliance to the established baseline security configurations, [redacted] and the [redacted] have an increased risk of becoming vulnerable to malicious attacks and system failure.

Without documentation evidencing essential internal control activities, vulnerabilities and control deficiencies may not be identified and thus could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] and [redacted] management to fulfill its mission requirements.

[redacted]

Without a procedure to document and review compliance checks to the established configuration baselines, the [redacted] system has an increased risk of becoming vulnerable to malicious attacks and/or system failure.

Without remediating critical- and high-risk vulnerabilities on a timely basis, [redacted] management cannot ensure the security and compliance of the [redacted] computing environment. System flaws 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]

Without a process to monitor system compliance to the established configuration baseline, there is an increased risk of the [redacted] system becoming vulnerable to malicious attacks and/or system failure.

Without reviewing vulnerability scans and remediating critical- and high-risk vulnerabilities on a timely basis, [redacted] management cannot ensure the security and compliance of the [redacted] system 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]

Without remediating critical-, high-, and medium-risk vulnerabilities on a timely basis, [redacted] management cannot ensure the security and compliance of the [redacted] 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.

We recommend [redacted]

4. Enforce controls to track all flaws and vulnerabilities in a POA&M that are discovered during security assessments or continuous monitoring and that cannot be remediated based on the defined flaw remediation timeline.

We recommend [redacted]

5. Design and implement policies and procedures for the baseline configuration review of [redacted] and [redacted] servers.
6. Maintain evidence of [redacted] and [redacted] baseline configuration reviews and compliance with established baselines.
7. Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the Flaw Remediation (SI-2) control is maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5, *Security and Privacy Controls for Information System and Organizations*.

We recommend [redacted]

8. Update configuration management related policies and procedures to include the process for the review of [redacted] system baseline configuration compliance checks.
9. Ensure [redacted] management conducts the review of baseline configuration compliance checks and maintains evidence of review.
10. Ensure all critical and high-risk vulnerabilities in the [redacted] environment are remediated in accordance with the timeframes established in the DOI SCS and, for vulnerabilities that cannot be remediated in accordance with policy, document a formal risk acceptance or develop a POA&M to document, evaluate, and accept the open vulnerabilities.

We recommend [redacted]

11. Design and implement a process to periodically review the [redacted] system baseline security configuration for compliance.
12. Design and implement a process to review vulnerability scans in accordance with DOI SCS.
13. Implement a mechanism to enforce the requirements outlined in the DOI RA and SI SCS for the [redacted] system.

We recommend [redacted]

14. Develop and implement corrective actions related to the [redacted] POA&Ms for the following four vulnerabilities:
    a. [redacted],
    b. [redacted],
    c. [redacted]
    d. [redacted].
15. Implement a mechanism to enforce the requirements outlined in the DOI RA and SI SCS for the [redacted].

3. Protect Function: Implementation of the IAM Program.

The table below lists deficiencies in the IAM program.

FISMA Metric Domain	Summary of Deficiencies
IAM	DOI established an IAM program; however, DOI did not ensure that: • Privileged user activity was logged and reviewed for the selected systems at [redacted], and [redacted]. • SOD controls were implemented for privileged users for one system at [redacted] • Privileged user access was reviewed at least annually for one system at [redacted] • Audit evidence for new user access forms and recertification documentation for privileged users for one system at [redacted] was available.

We performed the following procedures and noted the following deficiencies in the IAM programs of the following Bureaus and Offices: [redacted], and [redacted]

[redacted]

[redacted] management did not appropriately design and implement procedures for the review, analysis, and reporting of [redacted] audit logs for inappropriate or unusual activity on a weekly basis for the [redacted] system.

[redacted] management did not fully design and implement security controls to separate the functions of privileged users who support and administer the [redacted] system. Specifically, we noted the following:

- Two [redacted] privileged users who serve as database administrators and system architects had privileged access to the development environment and the production environment.
- Management did not require the review of privilege user activity by an individual who was independent of users whose activity was subject to review.

[redacted]

Audit evidence was not available for inspection to evaluate the design, implementation, and operating effectiveness of Account Management (AC-2) and Access Agreements (PS-6) security controls for the [redacted] system. As a result, these security controls were determined to be ineffective.

[redacted]

[redacted] system administrator activity was captured in audit logs; however, a review of administrator activity was not performed and documented in accordance with the DOI SCS.

[redacted]

System administrator activity for the [redacted] system was maintained in system audit logs; however, [redacted] management did not design and implement a process to review the administrator activity in accordance with the DOI SCS.

[redacted] management did not design and implement a process to review and reauthorize access for privileged user accounts, such as system administrators, for compliance in accordance with the DOI SCS.

DOI Security and Privacy Control Standards, Version 1.0, AU-2 Audit and Accountability (AU*):*
Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access ("data access" is usually referring to file and object access events), data changes, and permission changes.

b. Coordinate the event logging function with other organizational entities requiring audit- related information to guide and inform the selection criteria for events to be logged.

c. Specify the following event types for logging within the system: Password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, personal identity verification (PIV) credential usage, data action changes, query parameters, or external credential usage.

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging annually.

DOI Security and Privacy Control Standards, Version 1.0, AU-6 (AU)*:*
Control:

a. Review and analyze system audit records at least weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.

b. Report findings to designated organizational officials including but not limited to the SO, Information System Security Officer (ISSO), CISO, or ACISO based on severity; and

c. Adjust the level of audit record Review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

DOI Security and Privacy Control Standards, Version 1.0, AC-5 Separation of Duties
Control:

a. Identify and document System-Owner defined duties of individuals requiring separation; and

b. Define system access authorizations to support separation of duties

GAO, Standards for Internal Control in the Federal Government, dated September 2014, 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.

10.03 Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

DOI SCS, Access Control (AC), version 1.0, dated December 2022, AC-2 Access Management, 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 SCS, PS, version 1.0, dated December 2022, PS-6 Access Agreements, states:

The organization:

a. Develop and document access agreements for organizational systems;

b. Review and update the access agreements annually; and

c. Verify that individuals requiring access to organizational information and systems:

1. Sign appropriate access agreements prior to being granted access; and

2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or at a System Owner-defined frequency.

DOI SCS, 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

DOI System Security and Privacy Plan (SSPP) for [redacted], dated May 3, 2022, AU-2 Audit Events*:*

The organization:

a. Reviews [redacted] audit logs are daily and identifies suspicious events to be investigated immediately and, if not resolved by close of business reported to security.

[redacted] management did not identify or evaluate the risk associated with the lack of policies and procedures over the review of audit logs and user recertification procedures for [redacted] privileged users.

[redacted] management did not identify or evaluate the risk of potential abuse of authorized privileges or malicious user activity due to the lack of separation of duties. Additionally, we were informed that [redacted] did not have enough resources to effectively implement separation of duties processes.

[redacted]

Due to lack of internal communications within [redacted] and [redacted] management, [redacted] and [redacted] management were unable to provide sufficient audit documentation within the period designated by KPMG.

[redacted]

[redacted] management did not evaluate the risk associated with the lack of review of audit logs for the [redacted] system. Therefore, [redacted] management did not prioritize the review of audit logs for system administrators in accordance with DOI SCS.

[redacted]

[redacted] management did not evaluate the risk associated with failing to implement a process to review [redacted] system audit logs.

[redacted] management did not evaluate the risk associated with failing to implement a process to periodically review and reauthorize access for privileged user accounts.

[redacted]

Without the timely identification of unauthorized or otherwise inappropriate privileged user activity, unauthorized access and modification of data and computing resources could occur without management awareness.

Without the timely identification of unauthorized and/or inappropriate privileged user activity, unauthorized access and modification of data and computing resources could occur without management awareness.

[redacted]

Without documentation evidencing essential internal control activities, potential vulnerabilities and control deficiencies may not be identified and thus could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] and [redacted] management to fulfill its mission requirements.

[redacted]

Unauthorized access to and modification of the [redacted] system data and sensitive computing resources may occur without management's awareness.

[redacted]

Unauthorized access to and modification of the [redacted] system data and sensitive computing resources may occur without management's awareness.

When privileged user access and accounts are not reviewed periodically, there is an increased risk that inappropriate access may be maintained. As a result, unauthorized access, disclosure, and modification of the [redacted] system data and sensitive computing resources may occur.

We recommend [redacted]

16. Design and implement procedures to perform independent audit log reviews of the operating systems and web servers supporting the [redacted] system in accordance with DOI SCS.
17. Design and implement SOD policies and procedures for privileged users to ensure users with access to the development environment do not also have access to the production environment.
18. Design and implement policies and procedures to perform independent audit log reviews for all [redacted] privileged user activities in accordance with DOI SCS.

We recommend [redacted]

19. Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the AC-2 and PS-6 controls are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5. *Security and Privacy Controls for Information System and Organizations*.

We recommend [redacted]

20. Implement procedures to review the audit logs of system administrator activity in accordance with DOI SCS and the [redacted]-system policies and procedures.
21. Identify an audit log reviewer that is independent of the privileged users' activities noted in the audit logs.
22. Maintain evidence of privileged user activity reviews performed for the [redacted] system to include the reviewer's name and the date the review was performed.

We recommend [redacted]

23. Design and implement procedures to review and reauthorize privileged [redacted] system users access annually in accordance with the DOI SCS.

4. 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, [redacted] did not maintain audit evidence for DIT encryption for one system.

We performed the following procedures and noted the following deficiency in the [redacted] DPP program.

[redacted]

Audit evidence related to the NIST 800-5, Rev 5, System and Communication Protection (SC), Transmission Confidentiality and Integrity (SC-8) control was not available for inspection to determine its design, implementation, and operating effectiveness for the [redacted] system. As a result, the security control was determined to be ineffective.

GAO, Standards for Internal Control in the Federal Government, dated September 2014, 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.
10.03 Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

DOI SCS, SC, version 1.0, dated December 2022, SC-8 Transmission Confidentiality, and Integrity, states:

The organization:
a. Protect the confidentiality and integrity of transmitted information.

Due to the lack of internal communications within [redacted] and [redacted] management, [redacted] and [redacted] management were unable to provide sufficient audit documentation within the period designated by KPMG.

Without documentation evidencing essential internal control activities, management may not identify control gaps in its processes and procedures. Consequently, potential vulnerabilities and control deficiencies may not be identified and therefore could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] and [redacted] management to fulfill its mission requirements.

We recommend [redacted] management:

24. Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the SC-8 control are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5. *Security and Privacy Controls for Information System and Organizations*.

5. Respond Function: Implementation of the IR Program.

The table below lists deficiencies in the IR program.

FISMA Metric Domain	Summary of Deficiencies
IR	DOI established an IR program; however, DOI did not ensure that: • Incident tickets involving PII were reported to the US-CERT within one hour of discovery for the OCIO. • The Event Logging (EL) and retention program was operating at the EL1 maturity tier by August 27, 2022, and the EL2 maturity tier by February 27, 2023, for the OCIO.

We performed the following procedures and noted the following deficiencies in the OCIO IR program.

OCIO:

The DOI Computer Incident Response Center (CIRC) did not consistently implement processes to ensure that all PII related security incident tickets were reported to the US-CERT within one hour of discovery in accordance with the DOI SCS.

Of the 15 PII-related incident tickets inspected, two incidents were reported past the required one-hour timeline. One incident ticket was reported 21 hours past the one-hour timeline, and the second incident ticket was reported 13 minutes past the required timeline.

The DOI event log management and retention program were operating at the EL0 maturity tier. DOI did not fully implement the event logging and retention requirements specified within the OMB Memorandum M-21-31. Specifically, DOI did not implement the 12-month active storage and 18-month cold data storage requirements.

NIST SP 800-53, Rev. 4[1]*, U.S. DOI, OCIO, Security and Privacy Control Standard* – IR-6 Incident Reporting, states:

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

US-CERT Federal Incident Notification Guidelines, effective April 1, 2017, Notification Requirement, states*:*

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 Cybersecurity and Infrastructure Security Agency (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 IT department.

DOI OCIO, Enterprise Computer Security IR 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 NIST definition of an incident are required to be reported to DOI-CIRC within one hour of the determination.

OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, dated August 27, 2021, states:

The agency:

Must immediately begin efforts to increase performance in accordance with the requirements of this memorandum. Specifically, agencies must:

a. Within 60 calendar days of the date of this memorandum, assess their maturity against the maturity model in this memorandum and identify resourcing and implementation gaps associated with completing each of the requirements listed below. Agencies will provide their plans and estimates to their OMB Resource Management Office (RMO) and Office of the Federal Chief Information Officer (OFCIO) desk officer.

b. Within one year of the date of this memorandum, reach EL1 maturity.

c. Within 18 months of the date of this memorandum, achieve EL2 maturity.

d. Within two years of the date of this memorandum, achieve EL3 maturity.

Tier EL1, Rating – Basic

The agency and all of its components meet the following requirements, (*EL1 Basic Requirements*) within Appendix A (*Implementation and Centralized Access Requirements*):

- Basic Logging Categories
- Minimum Logging Data
- Time Standard
- Event Forwarding
- Protecting and Validating Log Information
- Passive DNS (Domain Name Service)
- CISA and Federal Bureau of Investigations (FBI) Access Requirements
- Logging Orchestration, Automation, and Response – Planning
- User Behavior Monitoring – Planning
- Basic Centralized Access

Tier EL2, Rating – Intermediate

The agency and all of its components meet the following requirements, as detailed in Table 3 (EL2 Intermediate Requirements) within Appendix A (Implementation and Centralized Access Requirements):

- Meeting EL1 maturity level
- Intermediate Logging Categories
- Publication of Standardized Log Structure
- Inspection of Encrypted Data
- Intermediate Centralized Access

- Data Retention Periods: 12-months active storage and 18-months cold data storage.

Due to a lack of consistent training and access to reporting guidelines, analysts were not knowledgeable of the timing requirements associated with reporting.

DOI OCIO management informed us that the current Security Information and Event Management (SIEM) tool has limited data storage capabilities, which prevented DOI from achieving full EL1 and EL2 compliance.

These conditions increase the risk that DOI will not be able to share relevant cybersecurity related logs to the CISA and FBI to address cybersecurity risks or incidents, as appropriate.

We recommend the DOI CIRC and Bureau/Office Security Analysts:

25. Implement a process to ensure that DOI CIRC analysts are trained to perform activities in alignment with the one-hour reporting requirement in accordance with the DOI SCS.

We recommend DOI:

26. Acquire the data storage needed to effectively implement the data retention requirements outlined in OMB M-21-31.
27. Enhance event log management policies and procedures to aid in the implementation of the requirements outlined in OMB M-21-31.
28. Establish a monitoring process to ensure all Bureaus and Offices have effectively implemented the revised event log management policies and procedures.

6. Recover Function: Implementation of the CP Program.

The table below lists deficiencies in the CP program.

FISMA Metric Domain	Summary of Deficiencies
CP	DOI established a CP program; however, [redacted] did not ensure that audit evidence for an information system contingency plan was available for inspection for one system.

We performed the following procedures and noted the following deficiency at [redacted]

[redacted]

The [redacted] information system contingency plan was not available for inspection to evaluate the design, implementation, and operating effectiveness of the Contingency Plan (CP-2) security control. As a result, the security control was determined to be ineffective.

GAO, Standards for Internal Control in the Federal Government, dated September 2014, 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.
> 10.03 Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained.

DOI SCS, CP, version 1.0, dated December 2022, CP-2 Contingency Plan, states:
The organization:

> a. Review the contingency plan for the system at least annually;
> b. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

Due to the lack of internal communications within [redacted] and [redacted] management, [redacted] and [redacted] management were unable to provide sufficient audit documentation within the period designated by KPMG.

Without documentation evidencing essential internal control activities, management may not identify potential vulnerabilities and control deficiencies that could lead to system compromise, data exposure, loss of data, reputational damage, and the inability for [redacted] and [redacted] management to fulfill its mission requirements.

We recommend [redacted] and [redacted] management:

29. Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the CP-2 control are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53 Rev 5. *Security and Privacy Controls for Information System and Organizations*.

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 NIST 800-53 security controls referenced in the FY 2023 IG FISMA Reporting Metrics. DOI did not fully design and implement the NIST SP 800-53, Rev 5, standards; therefore, we tested select security controls identified in the NIST SP 800-53, Rev 4, and additional security program areas identified in the FY 2023 Core and Supplemental IG Metrics. We identified control deficiencies associated with the areas of RM, CM, IAM, DPP, IR, and CP.

Based on the OMB's FY 2023 IG Metrics guidance and on the CyberScope results, DOI's information security program was assessed as not effective because the calculated average of the Cybersecurity Function Areas was 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 29 recommendations related to the control deficiencies we identified during the FISMA performance audit. If effectively implemented by management, these remediations should strengthen DOI's information security program.

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 accountable for consistent and effective execution of their security controls, as well the remediation of identified control deficiencies.

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

The DOI's Management Response to the FY 2023 OIG FISMA Performance Audit Report, 2023-ITA-008.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

November 28, 2023

Memorandum

To: Mark Lee Greenblatt
Inspector General

Through: Darren B. Ash
Chief Information Officer
Office of the Chief Information Officer

DARREN ASH Digitally signed by DARREN ASH
Date: 2023.11.28 12:27:17 -05'00'

From: Stanley F. Lowe
Chief Information Security Officer
Office of the Chief Information Officer

STANLEY LOWE Digitally signed by STANLEY LOWE
Date: 2023.11.28 09:08:01 -05'00'

Subject: Response to OIG Draft FY 2023 FISMA Report by Independent Public Auditor (2023-ITA-008)

Thank you for providing the Department of the Interior (Department, DOI) the Office of Inspector General (OIG) Draft Report on October 30th of the *Federal Information Security Modernization Act of 2014 Fiscal Year 2023 Performance Audit (2023–ITA–008).* This memorandum including attachment(s) will be emailed to aie_reports@doioig.gov as requested.

If you have questions, please contact Stan Lowe, Chief Information Security Officer, at [redacted]@ios.doi.gov and OCIO_Audit_Management@ios.doi.gov.

Attachment 1: Recommendations and Responses

cc: Naznin Rahman, Chief, Audit Management Division, Office of Financial Management
DOI Information Management and Technology Leadership Team
DOI Cyber Security Leadership Team
Richard Westmark, Chief, Compliance Management Section, OCIO

Attachment 1: Recommendations and Responses

The Department of the Interior's (Department, DOI) Management Response to the Fiscal Year (FY) 2023 Draft Office of Inspector General (OIG) Federal Information Security Management Act (FISMA) Performance Audit Report, 2023-ITA-008.

Below are the recommendations (**bold**) from the draft report; and bureau and office management responses (*italic*) from the draft report.

Recommendation 1. [redacted]: Ensure [redacted] management develop and implement processes and procedures that will ensure documentation and information related to the System Component Inventory (CM-8) control are maintained and available to address audit requirements as required by the [Government Accountability Office] GAO Standards for Internal Control in the Federal Government and [National Institute of Standards and Technology] NIST SP 800-53, Rev 5, *Security and Privacy Controls for Information System and Organizations.*

Response: Concur. *The [redacted] provided a system component inventory during the initial provided-by-client list gathering; however, [redacted] does not manage the software licenses for [redacted]. The DOI [redacted] purchases, distributes, and manages [redacted] software licenses. The [redacted] will contact DOI [redacted] to ensure that [redacted] licenses are properly tracked and assigned.*

System component inventories are maintained in the [redacted] tool, currently [redacted]. The [redacted] has provided a screenshot of the inventory in [redacted]

Target date: [redacted]
Responsible Official: [redacted] Associate Chief Information Security Officer (ACISO)

Recommendation 2. [redacted] Enhance the POA&M maintenance process to ensure that all bureau-level open [Plan of Action and Milestones] POA&Ms are reviewed and updated quarterly in accordance with DOI policy.

Response: Concur. *[redacted] Risk Management (RM) is developing [redacted] specific procedures for managing POA&Ms throughout their lifecycle. Once finalized, the RM POA&M Procedures document will be provided to Information System Security Officers (ISSOs). The ISSOs will be required to acknowledge receipt of the document and acknowledge that they have read and understand their responsibilities for managing POA&Ms throughout their lifecycle. Estimated completion date: [redacted].*

Target date: [redacted]
Responsible Official: [redacted] ACISO [redacted]

Response: Concur*. The Office of the Chief Information Officer (OCIO) will ensure the [redacted] tool is updated to require Severity Codes and Milestones to be mandatory fields in the POA&M entry screen prior to the POA&M being placed in 'Ongoing' Status.*

Target date: [redacted]
Responsible Official: [redacted] Chief Information Security Officer (CISO)

***Response: Concur**. The [redacted] concurs with the recommendation and plans to issue a POA&M management plan that will require the quarterly review and update of all open POA&Ms.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

***Response: Concur**. In addition to [redacted] response reported on page 39 of this report, [redacted] confirms remediation for recommendation (2) is tracked in [redacted] via a program-level POA&M, under the [redacted], with the CISO as the point of contact (POC). Further, [redacted] lists below CA-5 POA&M [redacted], Milestone #1 Completed Actions:*

- *The [redacted] POA&M review process has been enhanced which documents the requirement for a quarterly review of all open POA&Ms. The [redacted] developed a [redacted] procedures document for review and compliance of POA&M management. The procedures document and training has been provided to Information System Security Managers (ISSM)s and ISSOs. The document is also made available on the [redacted] Information Security Office (ISO) Compliance POA&M website page.*
- *The ISO Compliance POA&M Manager and team monitor and track completion of program-level and system-level open POA&Ms monthly. Subsequently, a quarterly review is performed, and a POA&M status report is provided to the ISSM, noting concerns. The ISSMs and ISSOs are required to monitor and track the completion of system-level open POA&Ms on a quarterly basis, to include an assessment and briefing to their system owners. Lastly, the [redacted] Authorizing Official (AO) is provided an overall status of POA&Ms on the quarterly Security Posture Briefing.*

Target date: Implemented [redacted]
Responsible Official: [redacted] ACISO [redacted]

Recommendation 3. [redacted]: Ensure all required fields such as milestone and scheduled completion dates are documented and defined for each open POA&M.

***Response: Concur.** [redacted] RM is developing [redacted] specific procedures for managing POA&Ms throughout their lifecycle. Once finalized, the RM POA&M Procedures document will be provided to ISSOs.*

The ISSOs will be required to acknowledge receipt of the document and that they have read and understand their responsibilities for managing POA&Ms throughout their lifecycle. Estimated completion date: [redacted]

Target date: [redacted]
Responsible Official: [redacted] ACISO [redacted]

***Response: Concur**. The OCIO will ensure the [redacted] tool is updated to require Severity Codes and Milestones to be mandatory fields in the POA&M entry screen prior to the POA&M being placed in 'Ongoing' Status.*

Target date: [redacted]
Responsible Official: [redacted], CISO

***Response: Concur**. The [redacted] concurs with the recommendation and plans to perform a check of all open POA&Ms for completeness as required by the [redacted] POA&M Management Plan.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

***Response**: **Concur**. In addition to [redacted] response reported on page 39–40 of this report, [redacted] confirms remediation for recommendation (3) is tracked in [redacted] via a program-level POA&M, under the [redacted], with the CISO as the POC. Further, [redacted] lists below CA-5 POA&M [redacted], Milestone #2 Ongoing Actions:*

- *Actions Being Completed: [redacted] developed a [redacted] procedures document for POA&M Management. The procedures document and training has been provided to ISSMs and ISSOs. The procedures document is also made available on the [redacted] ISO Compliance POA&M website page. The ISO Compliance POA&M Manager and team monitors and tracks the creation, updates, and completion of all bureau-level and system-level open POA&Ms, and as needed, discrepancy reports are provided to ISSMs for correction.*
- *The POA&Ms requiring updates and/or corrections are actively being addressed by ISSMs and ISSOs at this time. POA&Ms that cannot be updated/corrected by end of [redacted], will require a CA-5 System-level POA&M.*

Target date: [redacted]
Responsible Official: [redacted] ACISO [redacted]

Recommendation 4. [redacted]: Enforce controls to track all flaws and vulnerabilities in a POA&M that are discovered during security assessments or continuous monitoring, and that cannot be remediated based on the defined flaw remediation timeline.

***Response: Concur.** The [redacted] will develop procedures to track flaws and vulnerabilities in a POA&M when they are discovered during security assessments or continuous monitoring and cannot be remediated based on the defined flaw remediation timeline.*

Target date: [redacted]
Responsible Official: [redacted] Associate Chief Information Officer (ACIO)

Recommendation 5. [redacted] Design and implement policies and procedures for the baseline configuration reviews of [redacted] and [redacted] servers.

***Response**: **Concur.** The [redacted] will review its current guidance and update the [redacted] standard operating procedures to include guidance towards the baseline configuration of [redacted] servers in compliance with established DOI [redacted] policy. Additionally, [redacted] will update the [redacted] standard operating procedures to include the procedures and tools to conduct and maintain baseline configuration reviews. To track this effort, the [redacted] has established [redacted] POA&M [redacted] CM-06 Configuration Settings [redacted] Servers.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 6. [redacted] **Maintain evidence of** [redacted] **and** [redacted] **baseline configuration review and compliance with established baselines.**

Response: Concur*. The* [redacted] *will review its current guidance and update the* [redacted] *standard operating procedures to include guidance towards the baseline configuration of* [redacted] *servers in compliance with established DOI* [redacted] *policy. Additionally, the* [redacted] *will update the* [redacted] *standard operating procedures to include the procedures and tools to conduct and maintain baseline configuration reviews. To track this effort, the* [redacted] *has established* [redacted] *POA&M* [redacted] *CM-06 Configuration Settings* [redacted] *Servers.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 7. [redacted] **Develop and implement processes and procedures that will ensure** [redacted] **system documentation and information related to the Flaw Remediation (SI-2) control are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5,** ***Security and Privacy Controls for Information System and Organizations*****.**

Response: Concur. *The* [redacted] *will ensure that procedures are developed and implemented to address* [redacted] *flaw remediation. See* [redacted] *POA&M* [redacted] *SI-2 Flaw Remediation*

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 8. [redacted] **Update configuration management related policies and procedures to include the process for the review of** [redacted] **system baseline configuration compliance checks.**

Response: Concur. *The* [redacted] *will review and validate the current Change Control Procedures SOP to develop a procedure establishing a repeatable and standardized process regarding baseline configuration deviation review and compliance checks no later than* [redacted]

Target date: [redacted]
Responsible Official: [redacted] ACISO [redacted]

Recommendation 9. [redacted] **Ensure** [redacted] **management conduct the review of baseline configuration compliance checks and maintain evidence of review.**

Response: Concur. *The* [redacted] *will review and validate the current Change Control Procedures SOP to develop a procedure establishing a repeatable and standardized process regarding baseline configuration deviation review and compliance checks no later than* [redacted].

Target date: [redacted]
Responsible Official: [redacted] ACISO [redacted]

Recommendation 10. [redacted] Ensure all critical and high-risk vulnerabilities in the [redacted] environment are remediated in accordance with the timeframes established in the DOI [Security Control Standard] SCS and, for vulnerabilities that cannot be remediated in accordance with policy, document a formal risk acceptance or develop a POA&M to document, evaluate, and accept the open vulnerabilities.

Response: Concur. *The [redacted] has initiatives aimed at improving its ability to provide vulnerability management. These initiatives include, but are not limited to, refining policy and procedure, and establishing a repeatable and standardized process regarding vulnerability management. The [redacted] has updated the [redacted], created the [redacted] Risk Management POA&M Procedures, and introduced [redacted] which provides policy related to routine patching of software, applications, and firmware components of information systems utilized on the [redacted] network. The [redacted] states failure to follow patching requirements will lead to the system being temporarily removed from the network until remediation/mitigation is achieved. The [redacted] will complete and request closure of this Notice of Finding and Recommendation (NFR) no later than [redacted]*

Target date: [redacted]
Responsible Official: [redacted] ACISO [redacted]

Recommendation 11. [redacted]: Design and implement a process to periodically review the [redacted] system baseline security configuration for compliance.

Response: Concur. *The [redacted] management has taken immediate actions to improve its review of system baseline security configurations. POA&M [redacted] has been created to begin the design and implementation of a process to periodically review the [redacted] system baseline security configuration for compliance.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 12. [redacted] Design and implement a process to review vulnerability scans in accordance with DOI SCS.

Response: Concur. *The [redacted] management has taken immediate actions to improve its patch management processes and is in the process of implementing enterprise solutions to further automate control of its information technology asset inventory and to address patch management findings. The Enterprise Hosting Team and [redacted] Application Development Team remediated all the applicable vulnerabilities and subsequent scans noted their remediation. POA&M [redacted] has been created to start reviewing the DOI scans and implementing a mechanism to enforce the requirements in a timely fashion.*

Target date: Implemented [redacted]
Responsible Official: [redacted] ACISO

Recommendation 13. Implement a mechanism to enforce the requirements outlined in the DOI [Risk Assessment] RA and [System Integrity] SI SCS for the [redacted] system.

Response: Concur. *The [redacted] management has taken immediate actions to improve its patch management processes and is in the process of implementing enterprise solutions to further automate control of its information technology asset inventory and to address patch management findings. The Enterprise Hosting Team and [redacted] Application Development Team remediated all the applicable vulnerabilities and subsequent scans noted their remediation. POA&M [redacted] has been created to start reviewing the DOI scans and implementing a mechanism to enforce the requirements in a timely fashion.*

Target date: Implemented [redacted]
Responsible Official: [redacted] ACISO

Recommendation 14. [redacted] Develop and implement corrective actions related to the [redacted] POA&Ms for the following four vulnerabilities:

a) [redacted]
b) [redacted],
c) [redacted]
d) [redacted]

Response: Concur*.* [redacted] *concurs with the recommendation and will work with the application owner to remediate. Note that finding (A) has been remediated and a POA&M has been opened to track remediation of the remaining vulnerabilities.*

a) [redacted]
b) [redacted]
c) [redacted]
d) [redacted].

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 15. [redacted] Implement a mechanism to enforce the requirements outlined in the DOI RA and SI SCS for the [redacted] system.

Response: Concur. *The [redacted] Vulnerability Management and Patch Remediation Plan was just issued on December 16, 2022, and is still being implemented. [redacted] has just begun implementing the enterprise application vulnerability scanner and has prioritized internet-facing applications. [redacted] will continue to implement the processes detailed in the plan and implement the internal application scanning to proactively track application-level vulnerabilities.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 16. [redacted] Design and implement procedures to perform independent audit log reviews of the operating systems and web servers supporting the [redacted] system in accordance with DOI SCS.

Response: Concur. *[redacted] will develop and implement procedures to perform audit log reviews of the operating systems and web servers supporting the [redacted] system.*

Target date: [redacted]
Responsible Official: [redacted] ACIO

Recommendation 17. [redacted] Design and implement [Segregation of Duties] SOD policies and procedures for privileged users to ensure users with access to the development environment do not also have access to the production environment.

Response: **Concur.** [redacted] *will design and implement SOD procedures for privileged users based on DOI Security and Privacy Control Standards.*

Target date: [redacted]
Responsible Official: [redacted] ACIO

Recommendation 18. [redacted] Design and implement policies and procedures to perform independent audit log reviews for all [redacted] privileged user activities in accordance with DOI SCS.

Response: Concur. [redacted] *will develop and implement procedures to perform audit log reviews for [redacted] privileged user activities based on DOI Security and Privacy Control Standards.*

Target date: [redacted]
Responsible Official: [redacted] ACIO

Recommendation 19. [redacted] Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the AC-2 and PS-6 controls are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5, *Security and Privacy Controls for Information System and Organizations.*

Response: Concur. *The [redacted] will develop and implement procedures that will ensure documentation and information is available to address audit requirements upon request for [redacted]*

In response to the specific NIST Security Controls identified in this NFR:

AC-2 – Account Management

- *a) [redacted] has located the account management procedures for [redacted] and will provide them as part of the response to this NFR.*
- *b) [redacted] ensures that inactive accounts are disabled automatically in accordance with DOI requirements by identity management services provided by [redacted].*
- *c) [redacted] will develop and implement auditing procedures to ensure that all DOI audit logging and Reviewing requirements are met.*
- *d) [redacted] POA&M [redacted] AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-9: Audit Log Requirements*

PS-6 – Access Agreements

- *a) [redacted] meets the requirements for PS-6 by utilizing the DOI Rules of Behavior (ROB) for access agreements to all [redacted] information systems.*

Target date: [redacted]

Responsible Official: [redacted] ACISO

Recommendation 20. [redacted] Implement procedures to review the audit logs of system administrator activity in accordance with DOI SCS and the [redacted] -system policies and procedures.

Response: Concur. *The [redacted] will implement processes to review the audit logs of system administrator activity in accordance with DOI SCS and the [redacted] -system policies and procedures.*

Target date: [redacted]
Responsible Official: [redacted], System Owner

Recommendation 21. [redacted] Identify an audit log reviewer that is independent of the privileged users' activities noted in the audit logs.

Response: Concur. *The [redacted] will identify an audit log process to review the privileged users' activities noted in the audit logs.*

Target date: [redacted]
Responsible Official: [redacted], System Owner

Recommendation 22. [redacted] Maintain evidence of privileged user activity reviews performed for the [redacted] system to include the reviewer's name and the date the review was performed.

Response: Concur. *The [redacted] will develop a process to maintain evidence of privileged user activity reviews performed for the [redacted] system to include the procedure utilized and the date the review was performed.*

Target date: [redacted]
Responsible Official: [redacted], System Owner

Recommendation 23. [redacted] Design and implement procedures to review and reauthorize privileged [redacted] system users access annually in accordance with the DOI SCS.

Response: Concur. *The [redacted] management has taken immediate actions to improve its review and reauthorize privileged users. POA&M [redacted] been created to initiate the design and implementation of procedures to review and reauthorize privileged [redacted] user access annually in accordance with the DOI SCS. The process will document and maintain evidence of the completion of the privileged user access review and reauthorization.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 24. [redacted] Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the SC-8 control are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5, *Security and Privacy Controls for Information System and Organizations.*

Response: Concur. *The [redacted] will ensure that protections are implemented for transmission*

confidentiality and integrity of [redacted] data. See [redacted] POA&M [redacted] SC-08 –DIT - Transmission Confidentiality and Integrity.

Target date: [redacted]
Responsible Official: [redacted] ACISO

Recommendation 25. DOI [Cyber Incident Response Center] CIRC and Bureau and Office Security Analysts: Implement a process to ensure that DOI CIRC analysts are trained to perform activities in alignment with the one-hour reporting requirement in accordance with the DOI SCS.

***Response: Concur**. As part of the FY23 FISMA Audit, two tickets were identified that were not reported to the Cybersecurity and Infrastructure Security Agency (CISA)—formerly US-CERT—within the mandated one-hour reporting period. One incident was reported 13 minutes beyond the required one-hour period. The second incident was not reported until the following business day. This gap was the result of confusion whether the incident was truly reportable, caused by insufficient information present in the original incident ticket.*

The DOI-CIRC intends to perform the following actions to mitigate this finding in the future:

1. *DOI-CIRC will review documented procedures on reporting cybersecurity incidents to CISA for any necessary corrections or areas to streamline.*
2. *Existing mechanisms to notify cyber analysts when incidents are reportable will be reviewed and improved where possible. Additional redundant and secondary notifications mechanisms will be evaluated.*
3. *DOI-CIRC will ensure that all cyber analysts receive continuous refresher training, aiming for quarterly training at a minimum. Training dates and attendees will be documented for future audits.*
4. *Reporting incidents to CISA is currently a manual process and potentially prone to human error or delays. DOI will consult with CISA on the feasibility to support automated submission of incidents to CISA's reporting system.*
5. *The current process for determining when incidents are reportable to CISA relies on certain triggers that occur in DOI's [redacted] ticketing platform, based on how certain incident fields are set. DOI bureaus and offices security teams have the ability to create DOI-CIRC incident tickets, which can result in an incident being deemed reportable at ticket creation. However, there are circumstances where tickets have needed further review by DOI-CIRC before they should have been determined to be reportable. In some instances, incidents that were initially determined to be reportable were updated otherwise after further review by DOI-CIRC. DOI-CIRC will thoroughly review the existing incident workflow processes with the idea to propose eventual changes in how tickets are classified as reportable. Before tickets are officially deemed reportable, thus starting the one-hour security level agreement (SLA) period, DOI-CIRC will have an opportunity to review. These changes may require modifications to technology platforms, processes, and training, this requiring significant time develop and implement. Any changes to existing procedures will be fully documented and included in ongoing training.*

Target date: [redacted]
Responsible Official: [redacted], CISO

Recommendation 26. DOI: Acquire the data storage needed to effectively implement the data retention requirements outlined in [Office of Management and Budget] OMB M-21-31.

Response: Concur. *Management is awaiting fiscal 2024 appropriation to fund the acquisition for additional enterprise logging capacity, and subsequent annual funding to implement prioritized event logging management.*

Target date: [redacted]
Responsible Official: [redacted], CISO

Recommendation 27. DOI: Enhance event log management policies and procedures to aid in the implementation of the requirements outlined in OMB M-21-31.

Response: Concur. *The DOI will enhance event log policies and procedures to aid in the implementation of recommendation 26.*

Target date: [redacted]
Responsible Official: [redacted], CISO

Recommendation 28. DOI: Establish a monitoring process to ensure all Bureaus and Offices have effectively implemented the revised event log management policies and procedures.

Response: Concur. *The DOI will establish performance measures to monitor bureau and office implementation of recommendation 27.*

Target date: [redacted]
Responsible Official: [redacted], CISO

Recommendation 29. [redacted] Develop and implement processes and procedures that will ensure [redacted] system documentation and information related to the CP-2 control are maintained and available to address audit requirements as required by the GAO Standards for Internal Control in the Federal Government and NIST SP 800-53, Rev 5, *Security and Privacy Controls for Information System and Organizations.*

Response: Concur. [redacted] *will ensure that the* [redacted] *Contingency Plan is reviewed and updated in accordance with DOI requirements. See* [redacted] *POA&M* [redacted] *CP-2 Contingency Plan.*

Target date: [redacted]
Responsible Official: [redacted] ACISO

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

The following table summarizes the Cybersecurity Functions and associated Bureaus and Offices 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 2023 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]
Identify	-	-	X	-	X	-	-	X	X	-	X
Protect	-	X	X	-	X	X	X	X	-	-	-
Detect	-	-	-	-	-	-	-	-	-	-	-
Respond	-	-	-	-	-	-	-	-	X	-	-
Recover	-	-	X	-	-	-	-	-	-	-	-

Appendix II – Listing of Acronyms

Acronym	Definition
AC	Access Control
ACIO	Associate Chief Information Officer
ACISO	Associate Chief Information Security Officer
AICPA	American Institute of Certified Public Accounts
AO	Authorizing Official
AQD	Acquisitions Services Directorate
AU	Audit and Accountability
BCSIRT	Bureaus and Offices Computer Security Incident Response Team
BIA	Bureau of Indian Affairs
BIA	Business Impact Assessment
[redacted]	[redacted]
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
[redacted]	[redacted]
CA	Security Assessment and Authorization
[redacted]	[redacted]
CDM	Continuous Diagnostics and Mitigation
[redacted]	[redacted]
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIRC	Computer Incident Response Center
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer

Acronym	Definition
CM	Configuration Management
CMP	Configuration Management Plan
CP	Contingency Planning
CSAM	Cyber Security Assessment and Management
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerability and Exposures
DHS	Department of Homeland Security
DIT	Data in Transit
DOI	United States Department of the Interior
DNS	Domain Name Service
DP&P	Data Protection and Privacy
EL	Event Logging
EO	Executive Order
[redacted]	[redacted]
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
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
[redacted]	[redacted]
HR	Human Resource
HTTP	Hypertext Transfer Protocol
IA	Identification and Authentication

Acronym	Definition
IA	Information Assurance
IAM	Identity and Access Management
IBC	Interior Business Center
IG	Inspector General
[redacted]	[redacted]
IMT	Interior Information Management and Technology
IR	Incident Response
[redacted]	[redacted]
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
MS	Microsoft
[redacted]	[redacted]
NFR	Notice of Finding and Recommendation
NIST	National Institute of Standards and Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OFCIO	Office of the Federal Chief Information Officer
[redacted]	[redacted]
OIG	Office of Inspector General
[redacted]	[redacted]
OMB	Office of Management and Budget
OS	Office of the Secretary
OS	Operating System

Acronym	Definition
OSMRE	Office of Surface Mining Reclamation and Enforcement
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PS	Personnel Security
RA	Risk Assessment
REV	Revision
[redacted]	[redacted]
RM	Risk Management
RMO	Resource Management Office
ROB	Rules of Behavior
SA	System and Services Acquisition
SC	System and Communication Protection
SCRM	Supply Chain Risk Management
SCS	Security Control Standard
SI	System and Information Integrity
SIEM	Security Information and Event Management
SO	System Owner
SOC	Security Operations Center
SOD	Segregation of Duties
SOL	Office of the Solicitor
SOP	Standard Operating Procedure
SP	Special Publication
SQL	Structure Query Language
SSP	System Security Plan
SSPP	System Security and Privacy Plan

Acronym	Definition
ST	Security Training
STIG	Security Technical Implementation Guide
US	United States
US-CERT	US Computer Emergency Readiness Team
USGS	United States Geological Survey

Appendix III – FY 2022 Recommendation Status

We reviewed prior year findings and recommendations for which corrective actions had been completed by management. We did not review corrective actions that were in development or not fully implemented. Below is a summary table of the FY22 FISMA report recommendations and their respective status as of October 4, 2023.

Table 1. FY2022 FISMA Report Recommendations and Status as of September 21, 2023.
15 of 24 Recommendations are Open

Recommendation Description	Status Open/Closed and Target Completion Date
1. [redacted]: Establish and adhere to milestones to develop and formalize the DOI SCS and ensure new NIST SP 800-53 Rev. 5 security control requirements are incorporated.	Closed 04/07/2023
2. [redacted] Enforce processes and procedures to ensure system patches and updates for the [redacted] system are tested, approved, and appropriately documented prior to being deployed to the production environment.	[redacted]
3. [redacted] Enforce the documentation procedures to ensure that all testing and approval for security patches are documented for [redacted].	[redacted]
4. [redacted] Ensure all [redacted] production servers are reviewed and monitored for baseline configuration compliance.	[redacted]
5. [redacted] Ensure that the [redacted] baseline configuration for [redacted] is reviewed and updated in accordance with the DOI SCS.	[redacted]
6. [redacted] Ensure that the [redacted] and [redacted] baseline configurations are consistently monitored and reviewed, false-positive results are removed, and investigate the failed configuration checks, as needed.	[redacted]
7. [redacted] Investigate failed checks in the [redacted] and [redacted] baseline configuration compliance reports, as needed.	[redacted]
8. [redacted] Implement the corrective actions in POA&M [redacted] to include the completion and approval of the [redacted]	[redacted]
9. [redacted] Ensure all critical and high-risk vulnerabilities on the [redacted] system are remediated in accordance with the DOI SCS. For vulnerabilities that cannot be remediated in accordance with policy, document a formal risk acceptance or develop a POA&M to document, evaluate, and accept the open vulnerabilities.	[redacted]
10. [redacted] Implement a mechanism to enforce the requirements outlined in the DOI Risk Assessment and System Information Integrity SCS for [redacted]	Closed 08/09/2023

Recommendation Description	Status Open/Closed and Target Completion Date
11. [redacted] Implement a mechanism to enforce the requirements outlined in the DOI Risk Assessment and System Information Integrity SCS for [redacted]	Closed 08/02/2023
12. [redacted] Implement a mechanism to enforce the requirements outlined in the DOI Risk Assessment and System Information Integrity SCS for [redacted]	[redacted]
13. [redacted] Update standard operating procedures to ensure timely coordination of vulnerability reports, patching, and other appropriate actions in accordance with [redacted] vulnerability and configuration policies and control standards.	[redacted]
14. [redacted] Implement a mechanism to enforce the requirements outlined in the DOI Risk Assessment and System Information Integrity SCS for [redacted]	Closed 08/03/2023
15. [redacted] Remediate high and medium-risk [redacted] detection vulnerabilities in accordance with the DOI SCS for [redacted]	[redacted]
16. [redacted] Document a risk acceptance or POA&M for vulnerabilities, system flaws, and CVEs that are unable to be remediated within the established DOI policies.	Closed 08/03/2023
17. [redacted] Review the [redacted] Operating System repository configuration settings or monitor the [redacted] vendor website to ensure the [redacted] servers receive the appropriate security patches and updates timely in accordance with the DOI SCS.	Closed 08/03/2023
18. [redacted] Enforce the procedures to perform weekly audit log reviews to monitor for privileged [redacted] user activities, in accordance with the DOI SCS.	[redacted]
19. [redacted] Establish and implement procedures to review privileged [redacted] users on an annual basis in accordance with DOI policy and document completion of such review.	[redacted]
20. [redacted] Identify and formally document auditable events for the [redacted] servers in accordance with the DOI Audit and Accountability SCS.	[redacted]
21. [redacted] Continue to implement procedures that are outlined in the [redacted] procedural document.	Closed 05/26/2023
22. [redacted] Develop and implement the process and procedures to monitor weekly audit log reviews of privileged [redacted] user activities in accordance with DOI SCS and document completion of such reviews.	[redacted]

Recommendation Description	Status Open/Closed and Target Completion Date
23. [redacted] Enforce policies and procedures related to controls CA-6 and CA-7 to maintain a valid ATO for [redacted]	Closed 08/01/2023
24. [redacted] Implement an enforcement mechanism to ensure timely completion of activities required to maintain a valid ATO for [redacted]	Closed 08/01/2023

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: RM	
NIST SP 800-53, Rev 4: CA-3	System Interconnections
NIST SP 800-53, Rev 4: CA-5	POA&Ms
NIST SP 800-53, Rev 4: CA-7	Continuous Monitoring
NIST SP 800-53, Rev 5: 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	RA Policy and Procedures
NIST SP 800-53, Rev 4: RA-2	Security Categorization
NIST SP 800-53, Rev 4: RA-3	RA
NIST SP 800-53, Rev 4: PL-2	SSP
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	RM 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: SCRM	
NIST SP 800-53, Rev 4: PM-30	SCRM Strategy
NIST SP 800-53, Rev 4: SR-1	Policy and Procedures
NIST SP 800-53, Rev 4: SA-4	Acquisition Process
NIST SP 800-53, Rev 4: SA-5	System Documentation
NIST SP 800-53, Rev 4: SR-3	Supply Chain Controls and Processes
NIST SP 800-53, Rev 4: SR-5	Acquisition Strategies, Tools, and Methods
NIST SP 800-53, Rev 4: SR-6	Supplier Assessments and Reviews
NIST SP 800-53, Rev 4: SR-11	Component Authenticity
Cybersecurity Protect Function: CM	
NIST SP 800-53, Rev 4: CM-1	CM 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	CM Plan
NIST SP 800-53, Rev 5: SI-2	Flaw Remediation
Cybersecurity Protect Function: IAM	
NIST SP 800-53, Rev 4: AC-1	AC Policy and Procedures
NIST SP 800-53, Rev 5: 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	IA Policy and Procedures
NIST SP 800-53, Rev 4: SI-4	Information System Monitoring
NIST SP 800-53, Rev 4: PL-4	ROB
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 5: PS-6	Access Agreements
Cybersecurity Protect Function: DP&P	
NIST SP 800-53, Rev 4: SC-7	Boundary Protection
NIST SP 800-53, Rev 5: 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: ST	
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: ISCM	
NIST SP 800-53, Rev 4: CA-1	CA 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: IR	
NIST SP 800-53, Rev 4: IR-1	IR 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: CP	
NIST SP 800-53, Rev 4: CP-1	CP Policy and Procedures
NIST SP 800-53, Rev 5: CP-2	CP Plan
NIST SP 800-53, Rev 4: CP-3	CP Training
NIST SP 800-53, Rev 4: CP-4	CP 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 – Maturity Levels to the FY 2023 IG FISMA Reporting Metrics

This appendix describes our maturity levels to the FY 2023 IG FISMA Reporting Metric questions for the annual independent evaluation of DOI 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 are determined by a calculated average.

For each FISMA question assessed at maturity Level 1, 2, or 3, we explained 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: RM – Consistently Implemented (Level 3)
- Identify Function: SCRM – Defined (Level 2)
- Protect Function: CM – Consistently Implemented (Level 2)
- Protect Function: IAM – Managed and Measurable (Level 3)
- Protect Function: DP&P – Managed and Measurable (Level 3)
- Protect Function: ST – Consistently Implemented (Level 3)
- Detect Function: ISCM – Managed and Measurable (Level 3)
- Respond Function: IR – Consistently Implemented (Level 3)
- Recover Function: CP - 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. However, DOI's overall information security program was not effective as we identified deficiencies in each of the five Functions and nine Domains.

We assessed the cybersecurity Identify Function as Defined (Level 2) and the Protect, Detect, Respond, and Recover Functions 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?

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?

Maturity Level: Consistently Implemented (Level 3). The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization is making sufficient progress towards reporting at least 80% of its GFEs through DHS' CDM program.

[redacted] and [redacted] did not restrict network access for mobile devices with outdated software.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, DOI should enforce the capability to deny access to agency enterprise services when security and operating system updates have not been applied within a given period based on DOI policy.

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?

Maturity Level: Consistently Implemented (Level 3). The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for Executive Order (EO) EO-critical software and mobile applications, used in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization establishes and maintains a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.

[redacted] and [redacted] did not prevent the execution of unauthorized software for mobile devices. [redacted] lacked a documented process for the management and review of its software asset inventory.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring that the software assets, including EO-critical software and 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 DOI's ISCM strategy. For mobile devices, DOI and its Bureaus and Offices should enforce the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).

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?

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 organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization uses the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization uses 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] and [redacted] did not define metrics to consistently monitor the effectiveness of their risk management program and maintain the appropriate risk tolerance levels.

DOI and its Bureaus and Offices can improve their maturity levels by utilizing the results of its system level risk assessments, along with other inputs, to perform and maintain an organization-wide cybersecurity and privacy risk assessment. The result of this assessment should be documented in a cybersecurity risk register and serve as an input into the organization's enterprise risk management program. DOI and its Bureaus and Offices consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. DOI and its Bureaus and Offices should ensure that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.

7. To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?

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 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; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)?

Maturity Level: Defined (Level 2). Policies and procedures for the effective use of Plan of Action and Milestones (POA&Ms) have been defined and communicated. These policies and procedures address, at a minimum, the centralized tracking of security deficiencies, prioritization of remediation efforts, monitoring and maintenance, and independent validation of POA&M activities.

[redacted] and [redacted] did not properly maintain POA&Ms. Specifically, POA&Ms were missing milestones, scheduled completion dates were not updated, and milestone completion dates were not maintained. [redacted] and [redacted] did not establish metrics to measure the effectiveness of their POA&M management process.

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

9. To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?

Maturity Level: Consistently Implemented (Level 3). The organization consistently uses a cybersecurity risk register, or other comparable mechanism to ensure that information about risks is 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. Further, processes to share cybersecurity risk information are integrated with the organization's ISCM processes.

[redacted] and [redacted] did not define their specific risk tolerance level. This metric was not applicable for [redacted] as the metric is managed and maintained by a third-party vendor.

DOI and its Bureaus and Offices can improve their maturity levels by employing robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of cybersecurity risks across DOI.

The dashboard should present qualitative and quantitative metrics that provide indicators of cybersecurity risk. Cybersecurity risks should be integrated into enterprise level dashboards and reporting frameworks. DOI and its Bureaus and Offices should ensure that data supporting the cybersecurity risk register, or other comparable mechanism, are obtained accurately, consistently, and in a reproducible format and is used to:

- Quantify and aggregate security risks
- Normalize information across organizational units
- Prioritize operational risk response activities

10. To what extent does the organization use 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?

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.

[redacted] and [redacted] did not establish qualitative and quantitative metrics to measure the effectiveness of their risk management program.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring that cybersecurity risk management information is integrated into ERM reporting tools (such as a governance, risk management, and compliance tool), as appropriate.

12. To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?

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 developed SCRM policies and provided them to its Bureaus and Offices; however, Bureaus and Offices did not fully implement SCRM-related policies and procedures. As a result of the Fiscal Year (FY) 2021 FISMA Performance Audit, the Department instructed the Bureaus and Offices to implement SCRM-related policies and procedures by December 2023.

DOI and its Bureaus and Offices can improve its maturity level by fully implementing its SCRM strategy across the organization and use the strategy to guide supply chain analyses, communication with internal and external partners and stakeholders, and in building consensus regarding the appropriate resources for SCRM. Further, DOI and its Bureaus and Offices use lessons learned in the implementation to review and update its SCRM strategy in an organization defined timeframe.

13. To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

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 #11).
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 developed SCRM policies and provided them to its Bureaus and Offices; however, Bureaus and Offices did not fully implement SCRM-related policies and procedures. As a result of the Fiscal Year (FY) 2021 FISMA Performance Audit, the Department instructed the Bureaus and Offices to implement SCRM-related policies and procedures by December 2023.

DOI and its Bureaus and Offices can improve its maturity level by consistently implementing its policies, procedures, and processes for managing supply chain risks for Interior-defined products, systems, and services provided by third parties. Further, DOI and its Bureaus and Offices use lessons learned in implementation to review and update its SCRM policies, procedures, and processes in an organization defined timeframe.

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.

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 use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks.

DOI developed SCRM policies and provided them to its Bureaus and Offices; however, Bureaus and Offices did not fully implement SCRM-related policies and procedures. As a result of the FY 2021 FISMA Performance Audit, the Department instructed the Bureaus and Offices to implement SCRM-related policies and procedures by December 2023.

DOI and its Bureaus and Offices can improve their maturity level by ensuring that policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component. In addition, DOI and its Bureaus and Offices obtain sufficient assurance, through audits, test results, software producer self-attestation (in accordance with M-22-18), or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, DOI and its Bureaus and Offices maintain visibility into its upstream suppliers and can consistently track changes in suppliers.

19. To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?

Maturity Level: Defined (Level 2). The organization has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.

[redacted] did not consistently maintain baseline configurations for the in-scope system. [redacted] maintained an open POA&M for policies and procedures regarding the development and maintenance of configuration baselines. This metric was not applicable for [redacted] and [redacted] as this metric was implemented and managed by a third-party vendor.

DOI and its Bureaus and Offices can improve their maturity levels by employing automated mechanisms (such as application whitelisting and network management tools) to detect unauthorized hardware, software, and firmware and unauthorized changes to hardware, software, and firmware.

20. To what extent does the organization use configuration settings/common secure configurations for its information systems?

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] and [redacted] did not consistently implement policies and procedures to monitor secure configuration settings for the in-scope systems. [redacted] maintained an open POA&M for the lack of a documented process over security related configuration changes. This metric was not applicable to [redacted], and [redacted] as this metric was implemented and managed by a third-party vendor.

DOI and its Bureaus and Offices can improve their maturity levels by consistently implementing, assessing, and maintaining secure configuration settings for its information systems based on the principle of least functionality. Further, the organization consistently uses SCAP-validated software assessing (scanning) capabilities against all systems on the network (in accordance with BOD 23-01) to assess and manage both code-based and configuration-based vulnerabilities. DOI and its Bureaus and Offices use lessons learned in implementation to make improvements to its secure configuration policies and procedures.

21. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?

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], and [redacted] did not consistently perform vulnerability scans and remediate vulnerabilities in accordance with DOI Risk Management policies. This metric was not applicable for [redacted], and [redacted] as a third-party vendor was responsible for flaw remediation and patch management for the in-scope information system.

DOI and its Bureaus and Offices can improve their maturity levels by consistently implementing its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, DOI and its Bureaus and Offices patch critical vulnerabilities within 30 days and use lessons learned in implementation to make improvements to its flaw remediation policies and procedures. Further, for EO-critical software platforms and all software deployed to those platforms, DOI and its Bureaus and Offices use supported software versions.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) 3.0 program to assist in protecting its network?

Maturity Level: Managed and Measurable (Level 4). The organization, in accordance with OMB M-19-26, DHS guidance, and its cloud strategy is ensuring that its 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.

24. To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems?

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 all 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 did not document and define qualitative or quantitative metrics to measure the effectiveness of its vulnerability disclosure policy.

DOI and its Bureaus and Offices can improve its maturity level by monitoring, analyzing, and reporting on the qualitative and quantitative performance measures used to gauge the effectiveness of its vulnerability disclosure policy and disclosure handing procedures.

26. To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

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 extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?

Maturity Level: Consistently Implemented (Level 3). The organization is consistently implementing its ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the FICAM and CDM requirements, and incorporates applicable Federal policies, standards, playbooks, and guidelines. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.

[redacted], and [redacted] did not consistently implement automated mechanisms to manage the implementation of the ICAM program. Manual processes are used to review and manage user accounts.

DOI and its Bureaus and Offices can improve their maturity levels by integrating its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture. DOI and its Bureaus and Offices should use 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.

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?

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 uses more specific/detailed agreements for privileged users or those with access to sensitive information, as appropriate.

[redacted], and [redacted] did not implement automated mechanisms to manage and review non-privileged and privileged user access. [redacted] was unable to provide evidence to support the completion and maintenance of access agreements for the in-scope system. This metric was not applicable for [redacted] and [redacted] as this metric is implemented and managed by a third-party vendor.

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

30. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Maturity Level: Managed and Measurable (Level 4). All non-privileged users use strong authentication mechanisms to authenticate to applicable organizational systems and facilities [organization-defined entry/exit points]. To the extent possible, the organization centrally implements support for non-PIV authentication mechanisms in their enterprise identity management system.

31. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Maturity Level: Managed and Measurable (Level 4). All privileged users, including those who can make changes to DNS records, use 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?

Maturity Level: Defined (Level 2). The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking; inventorying and validating; and logging and reviewing privileged users' accounts.

[redacted] and [redacted] did not consistently implement audit log and Review policies and procedures. [redacted] and [redacted] maintained open POA&Ms related to the audit logging and Review of privileged user activity for their in-scope systems. [redacted] and [redacted] did not implement automated processes for account management.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. DOI and its Bureaus and Offices limit the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; and ensures that privileged user activities are logged and periodically reviewed.

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.

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

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?

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

[redacted], and [redacted] did not implement qualitative or quantitative performance measures to assess the effectiveness of its privacy activities.

DOI and its Bureaus and Offices can improve their maturity levels by monitoring and analyzing quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. DOI and its Bureaus and Offices should conduct an independent review of its privacy program and makes necessary improvements.

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?

- 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: Consistently Implemented (Level 3). The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.

[redacted] was unable to provide audit evidence to support the consistent implementation of privacy security controls. [redacted] maintained an open POA&M related to the enforcement of Data in Transit (DIT) and Data at Rest (DAR). DOI and its Bureaus and Offices can improve their maturity levels by ensuring the security controls for protecting PII and other DOI sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the DOI's ISCM strategy.

37. To what extent has the organization implemented security controls (e.g., Endpoint Detection and Response (EDR)) to prevent data exfiltration and enhance network defenses?

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 uses email authentication technology and ensures the use of valid encryption certificates for its domains. The organization consistently implements EDR capabilities to support host-level visibility, attribution, and response for its information systems.

DOI did not document and define qualitative or quantitative metrics to measure the effectiveness of data exfiltration and network defenses.

DOI and its Bureaus and Offices can improve their maturity level by analyzing qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. DOI and its Bureaus and Offices should also conduct exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, DOI and its Bureaus and Offices should monitor its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records. Further, DOI and its Bureaus and Offices has assessed its current EDR capabilities, identified any gaps, and is coordinating with CISA for future EDR solution deployments.

41. To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented 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.

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 use 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?

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 use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment?
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
- Deployment methods

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 did not establish qualitative or quantitative metrics to measure the effectiveness of security awareness and training strategies and plans.

DOI and its Bureaus and Offices can improve their maturity levels by monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. DOI and its Bureaus and Offices ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

47. To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?

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], and [redacted] did not established qualitative or quantitative metrics to measure the effectiveness of the ISCM strategy.

DOI and its Bureaus and Offices can improve their maturity levels by monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and makes updates, as appropriate. DOI and its Bureaus and Offices ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

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.

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?

Maturity Level: Managed and Measurable (Level 4). The organization uses the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. Organization authorization processes include automated analysis tools and manual expert analysis, as appropriate.

54. How mature are the organization's processes for incident detection and analysis?

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

DOI and its Bureaus and Offices did not meet the logging requirements of the maturity Event Logging (EL) 1 basic in accordance with OMB Memorandum M-21-31.

DOI and its Bureaus and Offices can improve their maturity levels by implementing the EL1 basic logging requirements in accordance with OMB Memorandum M-21-31.

55. How mature are the organization's processes for incident handling?

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.

DOI did not consistently report incidents involving PII to the U.S. Computer Emergency Readiness Team (CERT) in the required timeframe. Bureaus and Offices did not document and define qualitative and quantitative metrics to measure the effectiveness of the incident response program.

DOI and its Bureaus and Offices can improve their maturity levels by effectively reporting PII-related incidents timely to the US CERT and monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures.

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?

Maturity Level: Managed and Measurable (Level 4). The organization uses [redacted], and/or other comparable tools or services, to detect and proactively block cyber-attacks or prevent potential compromises.

58. To what extent does the organization use 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

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

DOI and its Bureaus and Offices did not define performance metrics to measure the effectiveness of their incident response technologies.

DOI and its Bureaus and Offices can improve their maturity levels by defining and evaluating the effectiveness of its incident response technologies and make adjustments to configurations and toolsets, as appropriate.

60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?

Maturity Level: Consistently Implemented (Level 3). Individuals are performing the roles and responsibilities that have been defined across the organization. The organization ensures that contingency training is provided consistent with roles and responsibilities to ensure that the appropriate content and level of detail is included.

[redacted] and [redacted] maintained open POA&Ms associated with their failure to maintain up-to-date information system contingency plans. This metric was not applicable for [redacted] and [redacted] as this metric was implemented and managed by a third-party vendor. [redacted] was unable to provide evidence to support the implementation of controls relevant to this metric.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

61. To what extent does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?

Maturity Level: Defined (Level 2). The organization has defined its policies, procedures, and processes for conducting organizational and system-level [redacted] and for incorporating the results into strategy and plan development efforts.

[redacted] and [redacted] did not design and implement procedures for integrating the results of the organizations business impact analyses with the enterprise risk management process. This metric was not applicable for [redacted] and [redacted] as this metric was implemented and managed by a third-party vendor. [redacted] and [redacted] maintained open POA&Ms for the lack of current business impact analyses.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring the results of organizational and system level business impact analysis are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, DOI and its Bureaus and Offices use the results of its business impact analysis in conjunction with their risk registers to calculate potential losses and inform senior level decision making.

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?

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

[redacted] was unable to provide evidence of a current contingency plan. This metric was not applicable for [redacted], and [redacted] as this metric was managed by a third-party vendor. [redacted] and [redacted] maintained an open POA&M for the lack of conducting information system contingency plan tests or exercises.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP. Furthermore, Bureaus and Offices should employ automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.

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?

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 use the information to make risk-based decisions.

DOI did not establish data collection and reporting processes to measure the effectiveness of recovery activities.

DOI and its Bureaus and Offices can improve their maturity levels by ensuring metrics on the effectiveness of recovery activities are communicated to relevant stakeholders and DOI and its Bureaus and Offices have ensured that the data supporting the metrics are obtained accurately, consistently, and in a reproducible format.

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

REPORT FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

The Office of Inspector General (OIG) provides independent oversight and promotes integrity and accountability in the programs and operations of the U.S. Department of the Interior (DOI). One way we achieve this mission is by working with the people who contact us through our hotline.

If you wish to file a complaint about potential fraud, waste, abuse, or mismanagement in the DOI, please visit the OIG's online hotline at **www.doioig.gov/hotline** or call the OIG hotline's toll-free number: **1-800-424-5081**

Who Can Report?

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement involving the DOI should contact the OIG hotline. This includes knowledge of potential misuse involving DOI grants and contracts.

How Does it Help?

Every day, DOI employees and non-employees alike contact the OIG, and the information they share can lead to reviews and investigations that result in accountability and positive change for the DOI, its employees, and the public.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act, and other applicable laws protect complainants. Section 7(b) of the Inspector General Act of 1978 states that the Inspector General shall not disclose the identity of a DOI employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the course of the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-DOI employees who report allegations may also specifically request confidentiality.