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

Audit

Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024

Report No. 2024-CTD-006

March 2025

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

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

MAR 24 2025

Memorandum

To: Darren Ash
Chief Information Officer

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

Subject: *Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024*
Report No. 2024-CTD-006

This memorandum transmits KPMG LLP's Federal Information Security Modernization Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2024. FISMA (Pub. L. No. 113-283) requires Federal agencies to have an annual independent evaluation 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 evaluation or has the discretion to elect that an independent external auditor perform the evaluation.

KPMG, an independent public accounting firm, performed DOI's FY 2024 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-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, dated December 4, 2023. 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
- Office of the Chief Information Officer
- Interior Business Center
- 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 supply chain risk management, configuration management, identity and access management, incident response, information security continuous monitoring, and security training. KPMG made 27 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 2024 Performance Audit Report

Prepared for: The Office of the Inspector General
As of: December 10, 2024

KPMG LLP
1801 K St. NW
Washington, DC

Table of Contents

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

December 10, 2024

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, Interior) information security program and practices for its information systems. We conducted our performance audit during the period of April 1, 2024, to March 31, 2025, and our results are as of August 23, 2024.

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.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objective of this performance audit was to evaluate the effectiveness of Interior's information security program and practices related to the financial and non-financial related systems.

We assessed Interior's information security program as Consistently Implemented (Level 3), which was ineffective according to OMB's FY 2023 - 2024 Inspector General FISMA Reporting Metrics (IG FISMA Reporting Metrics) guidance.

We made 27 recommendations related to these findings that, when implemented, should strengthen Interior's information security program if effectively addressed by management. We also evaluated the implementation of recommendations identified during the FY 2023 FISMA performance audit during our fieldwork testing period that ended on August 23, 2024. We determined that 15 of 29 recommendations remained open and that 14 recommendations were assessed as closed (see Appendix II – Status of 2023 Recommendations).

KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of Interior, Interior Office of Inspector General, Department of Homeland Security, Government Accountability Office, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

Background

FISMA

FISMA was passed by Congress and signed into law by the President in 2014. FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce risks to an acceptable level. The act assigns specific responsibilities to federal agencies, NIST, and the Office of Management and Budget (OMB) to strengthen federal information system security.

FISMA directs NIST to develop standards and guidelines for ensuring the effectiveness of information security controls over information systems that support federal agencies' operations and assets. In response to this mandate, NIST has developed a comprehensive risk-based management framework to guide agency efforts to establish effective information security management programs in compliance with FISMA. Specifically, the framework provides standards and guidelines for agencies in categorizing information systems, selecting security controls to meet minimum security requirements, performing risk and security controls assessments, authorizing systems into operations, performing monitoring activities to continually assess adequacy of security controls in supporting agency operations, and developing corrective action plans to mitigate security risks identified throughout a system's lifecycle.

Annually, agency IGs are required to either perform an independent evaluation or contract an independent external auditor to perform an evaluation of the agency's information security program and practices to evaluate the effectiveness of the program and practices. Each evaluation must include: (1) testing the effectiveness of information security programs and practices of a representative subset of the agency's information systems; (2) an assessment (based on the results of the testing) of requirements with FISMA; and (3) separate representations, as appropriate, regarding information security related to national security systems.

OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal Chief Information Officers (CIO) and Chief Information Security Officers councils, released OMB's guidance for implementing the requirements outlined in OMB Memorandum (M) 24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, outlined in the *FY 2023 – 2024 Inspector General FISMA Reporting Metrics* (IG FISMA Reporting Metrics). The IG FISMA Reporting Metrics are aligned with the five information security functions outlined in the *National Institute of Standards and Technology* (*NIST) Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. CIGIE maintained the maturity models for the following nine FISMA Metric Domains: Risk Management (RM), Supply Chain Risk Management (SCRM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP). **Table 1** illustrates the alignment of NIST Cybersecurity Framework to the FISMA Metric Domains within the IG FISMA Reporting Metrics.

Table 1: Alignment of NIST Cybersecurity Framework to the FISMA Metric Domains

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	Risk Management Supply Chain Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: IG FISMA Reporting Metrics.

Consistent with FY 2023, the metrics have five maturity levels: *Ad-hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Function.

Table 2: Inspector General 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.

Source: IG FISMA Reporting Metrics.

The IG FISMA Reporting Metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. The IG FISMA Reporting Metrics included Core Metrics and Supplement Metrics Group 2, as depicted in **Table 3.**

Table 3: FY 2024 Metric Scoping

Core Metrics	Supplemental Metrics Group 2
1 - System Inventory	4 - Enterprise Architecture and System Categorization
2 - Hardware Inventory	6 - Information System Security Architecture
3 - Software Inventory	15 - SCRM Counterfeit Components
5 - Enterprise Risk Management & Risk Assessments	17 - CM Roles and Responsibilities
10 - RM Dashboards and Reporting	18 - Enterprise-Wide Configuration Management Policy
14 - SCRM Processes	23 - Application Configuration Change Control
20 - Configuration Settings	28 - Personnel Risk Designations
21 - Flaw Remediation	38 - Data Breach Response Plan
30 - MFA - General Users	39 - Privacy Awareness Training
31 - MFA - Privileged Users	44 - Cybersecurity Awareness Training
32 - Privileged User Account Management	45 - Specialized Security Training
36 - Encryption	50 - ISCM Performance Measures
37 - Data Exfiltration and Network Defenses	52 - Incident Response Policies and Procedures
42 - Workforce Assessment	53 - IR Roles and Responsibilities and Training
47 - ISCM Strategy	56 - Incident Response Reporting and Communication
49 - ISCM Processes	62 - Information System Contingency Plan
54 - Incident Response Tools and Detection	64 – Backups
55 - Incident Response Tools and Handling	
61 - Business Impact Analysis	
63 - ISCP Test, Training, and Exercise	

Source: IG FISMA Reporting Metrics.

According to the IG FISMA Reporting Metrics guidance, a security program is considered effective if the calculated average of the metrics in a particular domain is Managed and Measurable (Level 4) or higher. For FY 2024, a calculated average scoring model was used in which Core Metrics and Supplemental Metrics Group 2 were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. The calculated averages of both the Core

Metrics and Supplemental Metrics Group 2 are used as data points to support the risk-based determination of overall program and function level effectiveness. Other data points considered include:

- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period;
- The progress made by agencies in addressing outstanding IG recommendations; and
- Reported security incidents reported during the review period.

IGs should use the CyberScope[1] reporting tool to calculate the maturity levels for each Cybersecurity Function and Domain and to submit the results of the IG Metrics evaluation. CyberScope provides supplementary fields to allow explanatory comments; IGs may use these fields to provide additional data supporting the Core Metrics evaluation results, and ultimately provide the overall effectiveness of the Interior's information security program.

Interior IT Organization

The Department's Office of the 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.

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

The Interior Chief Information Security Officer (CISO), also the Director of Cybersecurity within the OCIO, reports to the CIO and oversees the Cybersecurity Division. The Cybersecurity Division is responsible for IT cybersecurity and privacy at the Department level, to include governance, risk management, and incident response. The Cybersecurity Division provides a single point of accountability and visibility for cybersecurity, information privacy and security.

Each Bureau and Office 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 the Interior CISO.

The OCIO's mission and primary objective is to establish, manage, and oversee a comprehensive information management and technology program for the Interior. A stable and secure IMT environment is critical for achieving the Department's mission.

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

Objective, Scope and Methodology

Objective

The audit objective of our work was to provide an independent performance audit of Interior'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 objective.

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.

Scope

The scope of the performance audit was based on a subset of Interior's information systems across the following 11 Bureaus and Offices:

1. The **Bureau of Indian Affairs (BIA)** is responsible for the administration and management of 55 million surface acres and 57 million acres of subsurface minerals estates held in trust by the United States for American Indian, Indian tribes, and Alaska Natives.
2. The **Bureau of Land Management (BLM)** administers 262 million surface acres of America's public lands, located primarily in 12 Western States. The BLM sustains the health, diversity, and productivity of the public lands for the use and enjoyment of present and future generations.
3. The **Bureau of Reclamation (BOR)** manages, develops, and protects water and related resources in an environmentally and economically sound manner in the interest of the American public.
4. The **Bureau of Safety and Environmental Enforcement (BSEE)** is responsible for overseeing the safe and environmentally responsible development of energy and mineral resources on the Outer Continental Shelf.
5. The **U.S. Fish and Wildlife Service (FWS)** was created to conserve, protect, and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people.
6. The **National Park Service (NPS)** 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 **Office of the Chief Information Officer (OCIO)** provides leadership to the Interior and its bureaus in all areas of information management and technology. To successfully serve the Department's multiple missions, the OCIO applies modern IT tools, approaches, systems, and products. Effective and innovative use of technology and information resources enables transparency and accessibility of information and services to the public.
8. The **Interior Business Center (IBC)** is a federal shared service provider that offers Acquisition, Financial Management and Human Resources systems and services to federal organizations.

9. The **Office of Surface Mining Reclamation and Enforcement (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 **Office of the Solicitor (SOL)** performs the legal work for the Interior and manages the Departmental Ethics Office and the Departmental Freedom of Information Act (FOIA) Office.
11. The **U.S. Geological Survey (USGS)** serves the nation by providing reliable scientific information to describe and understand the earth; minimize loss of life and property from natural disasters; manage water, biological, energy, and mineral resources; and enhance and protect the nation's quality of life.

The subset of systems was selected in concurrence with the Interior Office of Inspector General (OIG) from the total population of information systems identified by management. National security systems were not within the scope of this performance audit. The population of systems consisted of 341 operational, FISMA reportable systems. We randomly selected 1 system at each of the 11 in-scope bureaus and offices which are listed below (**Table 4**). We did not include systems that were tested in FY 2023 or had a Low Federal Information Processing Standards (FIPS) 199 Category. In addition, the evaluation of management's corrective actions from prior year findings is considered in scope for the performance audit.

Table 4: Interior Information Systems Audited

#	Bureau/ Office	Information System	Bison Governance, Risk, and Compliance (BisonGRC) 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	OCIO	[redacted]	[redacted]	[redacted]

#	Bureau/ Office	Information System	Bison Governance, Risk, and Compliance (BisonGRC) ID	FIPS 199 Category
9	OSMRE	[redacted]	[redacted]	[redacted]
10	SOL	[redacted]	[redacted]	[redacted]
11	USGS	[redacted]	[redacted]	[redacted]

Methodology

We tested Interior's implementation of IT security controls as specified in NIST SP 800-53 Rev. 5.1.1, *Security and Privacy Controls for Information Systems and Organizations* and the IG FISMA Reporting Metrics. The performance audit focuses on assessing the design, implementation, and operating effectiveness of Interior's information security controls. As noted in **Table 1** above, these information security controls are based on five security functions: Identify, Protect, Detect, Respond, and Recover, which are derived from the NIST Cybersecurity Framework.

Our approach to accomplishing the FISMA performance audit was to evaluate the design, implementation, and operating effectiveness of the Interior's IT security program. We performed testing of security controls at the Department level, for the 11 Bureaus and Offices, and for 11 in-scope systems. Evaluating the design and implementation of the security controls entailed gaining an understanding of the FISMA related policies, procedures, practices, and guidelines established by the Interior and comparing them to the applicable federal laws and criteria.

In addition, when considering the use of information furnished by Interior management in the conduct of performance audit procedures, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluated whether the information was sufficiently precise and detailed.

Consistent with the FISMA Reporting Metric Guidance, a calculated average scoring model in which core metrics and supplemental metrics was averaged independently, was used to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. The calculated averages of the core and supplemental metrics were used as a data point to support the risk-based determination of overall program and function level effectiveness. Other data points considered included:

- The results of cybersecurity evaluations conducted by independent parties,
- The progress made by the Interior to remediate outstanding IG recommendations; and,
- Reported major security incidents reported during the audit period.

Results

Summary of Results

Table 5: Summary of Results per Cybersecurity Function and FISMA Metric Domain

Cybersecurity Framework Security Functions and FISMA Metric Domains	Summary of Results
1. Identify (RM and SCRM)	The Interior established RM and SCRM programs, and we did not identify and report any RM deficiencies. However, for its SCRM program, the Interior did not ensure that: • Anti-counterfeit controls were formally developed and implemented, and component authenticity and anti-counterfeit training was provided for designated personnel at the Interior. • The SCRM program was fully designed and implemented across the organization to include all bureaus and offices at the Interior.
2. Protect (CM, IAM, DPP, and ST)	The Interior established a CM, IAM, and ST program, and we did not identify and report any DPP deficiencies. However, for its CM, IAM and ST programs, the Interior did not ensure that: • Critical- and high-risk vulnerabilities were remediated within the Interior required timeframe for one system at [redacted]. • The appropriate controls for change management policies and procedures were implemented to ensure all configuration changes are documented, tested, and approved for one system at [redacted]. • Privileged user activity was logged and reviewed for the selected systems at [redacted], [redacted], [redacted], [redacted], and [redacted]. • Access and account management policies and procedures were defined, documented, and implemented for one system at [redacted]. • Privileged user access was reviewed at least annually for selected systems at [redacted], [redacted], and [redacted]. • Supporting documentation evidencing new privileged user access one system at [redacted] was available. • Network access was removed for users that did not complete their annual Role-Based Security Training (RBST) at [redacted].

Cybersecurity Framework Security Functions and FISMA Metric Domains	Summary of Results
3. Detect (ISCM)	The Interior established an ISCM program; however, the Interior did not ensure that: • Program measures used to assess the effectiveness of the Interior's ISCM program were defined to include the frequency of the collection and individuals responsible for the review. • The System Security and Privacy Plan (SSPP) for one system was signed and approved by the system owner and designated authorizing officials at [redacted].
4. Respond (IR)	The Interior established an IR program; however, the Interior did not operate the Event Logging (EL) and retention program at the [redacted][2] maturity tier and the [redacted][3] maturity tier for the Department.
5. Recover (CP)	The Interior has established an CP program, and we did not identify and report any deficiencies.

Based on the maturity levels calculated in CyberScope, we determined the Interior's information security program was not effective as it was not aligned with applicable FISMA requirements, Office of Management and Budget (OMB) policy and guidance, and NIST standards and guidelines. According to OMB's IG FISMA Reporting Metrics, a security program is considered effective if the calculated average of the metric 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) as noted in **Table 6**.

Table 6: Maturity Levels for Cybersecurity Functions

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

Refer to Appendix V, *Responses to the IG FISMA Reporting Metrics*, for the assessed maturity levels for each of the Core Metrics and Supplement Metrics Group 2.

We made 27 recommendations related to control deficiencies identified during our performance audit that,

[2] According to OMB M-21-31, [redacted] is one of four event logging tiers. [redacted]

[3] According to OMB M-21-31, [redacted] is one of four event logging tiers. [redacted]

if effectively implemented by the Interior, should strengthen the Interior's information security program.

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

Furthermore, the Interior 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 four appendices. Appendix I summarizes the program areas in which Bureaus and Offices have control deficiencies, Appendix II provides the status of FY 2023 recommendations, Appendix III lists the NIST SP 800-53 security controls cross-referenced to the Cybersecurity Framework, and Appendix IV provides the responses to the IG FISMA Reporting Metrics.

Results for FISMA Metric Domains

1. Identify Function: Implementation of the SCRM Program.

The table below summarizes the deficiencies in the SCRM program.

FISMA Metric Domain	Summary of Deficiencies
SCRM	The Interior established a SCRM program; however, the Interior did not ensure that: • Anti-counterfeit controls were formally developed and implemented, and component authenticity and anti-counterfeit training was provided for designated personnel. • The SCRM program was fully designed and implemented across the organization to include all bureaus and offices.

We noted the following deficiencies in the Interior SCRM program.

Interior:

The Interior did not formally develop and implement anti-counterfeit policies and procedures and did not provide component authenticity and anti-counterfeit training for designated personnel.

The Interior did not fully design and implement the SCRM program across the organization to include all bureaus and offices. Specifically:

1. 3 of 11 bureaus/offices did not fully design SCRM policies and procedures for their bureau/office-level SCRM program.
2. 11 bureaus/offices evaluated did not implement a program for assessing and reviewing the supply chain-related risks and evaluating security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization.

NIST SP 800-161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, Awareness and Training (AT), control AT-3 Role-Based Training:

Addressing cyber supply chain risks throughout the acquisition process is essential to performing C-SCRM effectively. Personnel who are part of the acquisition workforce require training on what C-SCRM requirements, clauses, and evaluation factors are necessary to include when conducting procurement and how to incorporate C-SCRM into each acquisition phase.

DOI Security and Privacy Control Standards Supply Chain Risk Management (SR), version 1.0:

Control SR-2 Supply Chain Risk Management Plan:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services];
b. Review and update the supply chain risk management plan [Assignment: organization defined frequency] or as required, to address threat, organizational or environmental changes; and
c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Control SR-3 Supply Chain Controls and Processes:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];
b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [Assignment: organization-defined supply chain controls]; and
c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization defined document]].

Control SR-11 Component Authenticity:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
b. Report counterfeit system components to DOI CISO, ACISO, and procurement offices; DOI Cyber Incident Response Center (DOI-CIRC) and bureau Computer Security Incident Response Team (CSIRTs).

DOI Information & Communications Technology (ICT) SCRM Strategy, v*ersion 1*:

Creation/update, as necessary, and documentation of controls and requirements not covered in NIST 800-53 or NIST SP 800-161 to detect, assess and respond to counterfeit and/or compromised systems and/or components in the ICT supply chain.

At each Tier, training will be provided to staff and individuals with staff-like access to educate them on their role with regard to ICT SCRM, define what ICT SCRM actions they are responsible for, and identify where to go and whom to contact to obtain further guidance, information and resources.

Section 3.2.1
The ICT SCRM OG, working in conjunction with the ERM function, determines the Department's ICT risk appetite and translates it into risk tolerance thresholds that are relevant and tangible to the Department, the Bureaus/Offices, and the System-level programs that they are responsible for. The Department's risk tolerance thresholds are captured in the Enterprise Cybersecurity Risk Management (ECRM) Plan. These risk tolerance thresholds should be taken as requirements by Tiers 2 and 3 when developing their ICT SCRM Plans. Additionally, as Framing is an ongoing process, the responsible parties at all tiers must updated their ICT SCRM Plans with guidance for the other steps in the ICT SCRM process (assess, respond, and monitor), as appropriate, based on the outputs of their framing activities.

Section 3.2.3
One of the most critical outputs of the Respond step is the formalization of the ICT SCRM Plan. The Department will generate and implement an ICT SCRM Plan, each Bureau/Office will generate and implement their own plan, and the Systems Owners for covered systems will generate and implement an ICT SCRM Plan. This Strategy provides the guidance for gathering all the data needed to create a comprehensive plan. These plans will govern how risk is addressed, at each tier, and ensure that the activities undertaken are sufficient to appropriately handle risks to the Department as well as the Bureaus/Offices and their subordinate systems. ICT SCRM Plans at all tiers are informed and governed by the risk context, risk decisions, and risk activities taken in the Frame and Assess steps. The ICT SCRM Plans must include:

- A summary of the applicable ICT environment as determined in Frame step; this includes, as applicable, policies, processes, laws, and procedures based on the Department and mission requirements it has currently implemented
- A statement of the role responsible for the approval and enforcement of the plan (i.e. CISO, Risk Executive, CIO, Program Manager, System Owner)
- Identification of key contributors such as the CIO, CISO, Bureau/Office Chief, Acquisition/Contracting, Program Managers, Operations Managers, System Architects
- Applicable controls resulting from the analysis of alternatives conducted in the Respond step, including but not limited to the NIST SP 800-161 controls (NOTE: NIST provides controls at the Tier 1, Tier 2 and 3 levels, which should be addressed by their corresponding plans)
- Tailoring decisions for the selected controls including the rationale for the decision
- Selection of the applicable NIST SP 800-161 Tier 2 controls that the Department will pass on to its Tier 2 Bureau/Office-level programs as ICT SCRM requirements
- Creation/update, as necessary, and documentation of controls and requirements not covered in NIST 800-53 or NIST SP 800-161 to detect, assess and respond to counterfeit and/or compromised systems and/or components in the ICT supply chain
- Cost, schedule, and performance factors and constraints as well as a critical non-functional requirement such as reliability, dependability, safety, security, and quality.
- A reference and pointer to the listing of all key ICT suppliers that are applicable to the plan and the assessments of the suppliers' risk profiles
- When available, a reference to the Department-wide database of vendors/suppliers with the assessments of their capabilities and risk as executed by other programs within the Department; include the location of where to find the database and how to gain access
- A list of tools and technologies to assist in reviewing and evaluating new and existing suppliers
- Establishment of frequency, timeline, and triggering events for reviewing existing suppliers for ICT supply chain risk
- Documented guidance and verbiage, as appropriate, for inclusion in contracts, purchase

orders and other forms of procurements and/or acquisitions to ensure that vendors, subcontractors, and other program contributors, external to the Department, meet their requirements in a manner that supports the ICT SCRM goals and program missions

- Descriptions of the feedback processes between tiers including from Tier 1 back to the enterprise level to ensure ICT supply chain interdependencies are addressed
- Establishment of a frequency, timeline, and triggering events for deciding whether the plan needs to be revised

Interior:

Due to priority placed on acquiring a software tool to help streamline the SCRM program, the Department did not focus on other aspects of the SCRM program, such as anti-counterfeit controls.

Due to competing priorities and reliance placed on the Department, the bureaus and offices did not focus on the overall development of their respective SCRM programs. Additionally, the Department did not effectively monitor and enforce compliance with the Department-wide SCRM policy.

Interior:

The lack of a fully implemented SCRM program increases the risk of the risk of vulnerabilities being introduced into the Interior environment through external providers that provide products, systems, and services, thereby exposing the systems of the Interior and its Bureaus and Offices to threats and exposures.

We recommend Interior:

1. Develop and implement enterprise-wide policies and procedures to detect and prevent counterfeit components from entering the environment.
2. Develop and provide component authenticity and anti-counterfeit training to all designated personnel at least annually or a frequency defined by the Interior.
3. Oversee Bureaus and Offices to make sure that they implement their own SCRM policies and procedures respective to their unique risks in a documented and approved plan, which will be structured based on the Interior SCRM Strategy.
4. Implement a process to consistently assess and review the supply chain-related risks through evaluation that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet applicable regulations across all bureaus and offices.
5. Develop and implement a Department-level monitoring and enforcing process to ensure compliance with the overall SCRM program policies.

2. Protect Function: Implementation of the CM Program.

The table below summarizes the deficiencies in the CM program.

FISMA Metric Domain	Summary of Deficiencies
CM	The Interior established a CM program; however, the Interior did not ensure that: • Critical- and high-risk vulnerabilities were remediated within the Interior required timeframe for one system at [redacted]. • The appropriate controls for change management policies and procedures were implemented to ensure all configuration changes are documented, tested, and approved for one system at [redacted].

We noted the following deficiencies in the [redacted] CM Program.

[redacted]:

The October 2023 and May 2024 [redacted] reports for the [redacted] system identified a total of [redacted] vulnerabilities; however, management did not remediate the 2 vulnerabilities within [redacted] days and [redacted] days, respectively, which did not adhere to Interior policies. Additionally, [redacted] management did not formally document a risk-based decision and obtain approval of the risk acceptance as required by Interior policies. Specifically, the table below identifies critical and high-risk vulnerabilities not remediated timely.

System	[redacted] Plugin Identifier	Plugin Name	Severity	First Discovered	Last Observed	Days outstanding after the expected remediation period
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted] management did not have appropriate controls in place for the implementation of the configuration management process to ensure all configurations changes, regardless of impact level, were documented in a Bison System Support (BSS) ticket, tested, and approved as required by the

[redacted] documented process. Specifically, for the one configuration change implemented into production in FY 2024, the change was communicated via email, was not formally approved, and was not properly documented in a BSS ticket.

DOI Security and Privacy Control Standards System and Information Integrity (SI), version 1.0, control SI-2 Flaw Remediation:

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

DOI Security and Privacy Control Standards CM, version 1.0, control CM-3(2) Configuration Change Control:

Tests, validates, and documents changes to the information system before implementing the changes on the operational system.

[redacted] *Configuration Management Plan* [redacted]:

[redacted] Creating and Working Change Requests in the Bison Support System No Impact Change Request:

1. Change submitted as No Impact Change type using the [redacted] – Change Request (IT Only) form
2. System updates Status to Request for Change
3. Request is sent for Change Manager approval
4. System updates Status to Scheduled
5. Change Coordinator should now edit the request and can begin implementing the change based on the approved tasks, date, time, and plan
    a. Required: Add Change Coordinator Name
    b. Required: Update Status to Implementation in Progress
6. Once the change is implemented, Change Coordinator should edit the request:
    a. Required: Update Status to Completed
    b. Required: Add dates/times for Actual Start Date and Actual End Date the change took place
7. System updates Status Reason to Final Review Required
8. System updates Status Reason to Final Review Complete

[redacted] *Vulnerability Management Standard*:

Vulnerabilities can be remediated through:

- Patching – if a patch exists to address a specific vulnerability or set of vulnerabilities, it should be tested and applied to all applicable systems.
- Configuration changes – if a configuration change is needed to address a specific vulnerability or set of vulnerabilities, it should be submitted for approval through the configuration management process and applied to all applicable systems.
- Risk Acceptance – if the recommended fix cannot be applied, a Risk-Based Decision should be documented.

Remediation Time Frames:

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

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

[redacted]:

Due to lack of accountability, [redacted] management did not document a formal risk acceptance based on the type of risks associated with the vulnerabilities and its impact on the operational nature of the system. Furthermore, [redacted] did not have an oversight process to determine compliance with its vulnerability management standard.

[redacted] control operators were not aware of the requirement that all changes, including 'no impact' changes, must be documented through BSS tickets.

[redacted]:

Without remediating [redacted] vulnerabilities on a timely basis, [redacted] management cannot ensure the security and compliance with Interior and [redacted] policies for the system's 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.

Critical errors, system compromises, and/or disruption of services could occur if system changes are not appropriately approved and tested and the change process is not followed and documented, and such documentation is not retained, as required.

We recommend [redacted]:

6. Remediate [redacted] vulnerabilities on the [redacted] system in accordance with the timeframes established in applicable Interior Security Control Standards and [redacted] policies.
7. Implement an oversight process that provides accountability for system owners to remediate vulnerabilities timely or obtain risk acceptances, as appropriate.
8. Improve the implementation for all configuration changes to make control owners formally aware of the process and abide by the required change process workflow based on the type of change. [redacted] management should review the change made to the [redacted] environment in FY 2024 to confirm that it did not have an adverse impact on [redacted] functionality.

3. Protect Function: Implementation of the IAM Program.

The table below summarizes the deficiencies in the IAM program.

FISMA Metric Domain	Summary of Deficiencies
IAM	The Interior established an IAM program; however, the Interior did not ensure that: • Privileged user activity was logged and reviewed for the selected systems at [redacted], [redacted], [redacted], [redacted], and [redacted]. • Access and account management policies and procedures were defined, documented, and implemented for one system at [redacted]. • Privileged user access was reviewed at least annually for selected systems at [redacted], [redacted], and [redacted]. • Supporting documentation evidencing new user privileged access for one system at [redacted] was available.

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

[redacted]:

Although [redacted] had the capability to log activities and management used this capability to investigate activity as needed, [redacted] management did not implement procedures for the routine review of audit logs that capture privileged user activity to identify and follow up on potential incidents as required by Interior Security Control Standards.

For one of four new privileged users that were provisioned access to [redacted], the approval of the user's account was not appropriately documented through the current request and approval process using the [redacted]. When this was identified, a [redacted] system administrator revoked the user's access and required the user to resubmit an access request through [redacted].

[redacted]:

[redacted] [redacted] management did not complete the annual [redacted] access review and re-authorization, including privileged users, in accordance with Interior and [redacted] policies. Specifically, [redacted] did not complete the access recertification for any of the [redacted] users with administrative access to the system.

[redacted] [redacted] management did not consistently complete the weekly privileged user audit log reviews for the [redacted] system, in accordance with Interior and [redacted] policies and procedures. Specifically, [redacted] did not complete the privileged user audit log reviews for four of five weeks selected for testing. Additionally, for the one weekly privileged user activity review performed, the reviewer was not independent from the activity.

[redacted]:

[redacted] management did not complete its annual account access review and re-authorization for [redacted] in accordance with Interior policies. Specifically, [redacted] management did not complete the access review and re-authorization for [redacted] of [redacted] privileged user accounts selected for testing. Additionally, [redacted] management did not document procedures for completing a review of [redacted] privileged accounts in accordance with Interior policies.

[redacted]:

[redacted] management did not define, document, and implement a process to review the activity of privileged [redacted] users in accordance with Interior Security and Privacy Control Standards. As a result, management only reviewed the [redacted] audit logs of privileged users on an ad hoc basis.

[redacted] management did not design and implement a process to document the authorization of new privileged access for [redacted] in accordance with Interior policies. Specifically, management was unable to provide supporting documentation evidencing supervisor review and approval of new [redacted] privileged user access requests for FY 2024.

[redacted]:

[redacted] management did not define and document policies or procedures for access and account management for the [redacted]. Specifically, [redacted] management did not establish procedures that document how privileged user access should be requested, authorized, disabled and removed, and reviewed and re-authorized to include considerations of least privilege.[4] Additionally, no documented procedures existed for the frequency in which accounts should be reviewed and re-authorized, the supervisor responsible for completing the re-authorization, or the documentation and retention of the supervisor's signature to include the date the re-authorization was performed. Note: as of June 6, 2024, [redacted] management defined and documented a privileged and non-privileged account procedure to address this condition. KPMG noted the procedure included steps for requesting, authorizing, disabling/removing, and re-authorizing all user accounts.

[redacted] management did not define, document, or implement a process to log and review the activity of privileged users of the [redacted] in accordance with Interior Security and Privacy Control Standards. As a result of this finding, [redacted] re-opened Plan of Action and Milestones (POA&M) #[redacted] to track the remediation efforts related to the implementation of audit logging capabilities.

[redacted]:

[redacted] management provides support for the use of [redacted] to capture audit activity and investigate incidents. [redacted] management did not configure the tool to review privileged-use activity in accordance with the Interior IT Security and Privacy Control Standards and [redacted] procedures. [redacted] management has since configured the tool to perform that notification.

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

Control AU-2 Event Logging:
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,

[4] According to NIST SP 800-53, Rev. 5.1.1, least privilege is the principle of allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

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.

Control AU-6 Audit Record Review, Analysis, and Reporting:
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 System Owner (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 Access Control (AC), version 1.0:

Control AC-1 Policies and Procedures:

a. Develop, document, and disseminate to all stakeholders as defined by the Department, Bureaus, and Offices:
    1. Any organization-level, mission/business process-level, and system-level access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures to facilitate the implementation of the access control policy and the associated access controls;
b. Designate the CISO and Departmental Privacy Officer (DPO) at the Department level to develop access control policy and procedures for the enterprise, and Authorizing Officials (AOs), SOs, ISSOs at all levels as necessary to coordinate with Bureau/Office ACISOs and Associate Privacy Officers (APOs) to manage the development, documentation, and dissemination of the access control policy and procedures; and
c. Review and update the current access control:
    1. Policy according to the Bureau or System Information Security Continuous Monitoring Plan (ISCMP) (Note that a POA&M will be created if no ISCMP exists; the ISCMP is required for Assessment and Authorization [A&A]), and following applicable assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    2. Procedures as defined in the Bureau or System ISCMP and following applicable assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines.

AC-2 *Account Management*:

a. Define and document the types of accounts allowed and specifically prohibited for use within the system;
b. Assign account managers;
c. Require Bureau or system account management procedures that have prerequisites and criteria for group and role membership;
d. Specify:
    1. Authorized users of the system;

2. Group and role membership; and
3. Access authorizations (i.e., privileges) and Bureau or system account management procedures that have (required if appropriate) attributes for each account;

e. Require approvals by user's supervisor, system owner or any other managers as appropriate for requests to create accounts;
f. Create, enable, modify, disable, and remove accounts in accordance with system owner-defined procedures or conditions.
g. Monitor the use of accounts;
h. Notify account managers and sponsor, supervisor, contracting officer's representative (COR), or other roles/personnel listed in Bureau or system account management procedures and on/off-boarding procedures within:
    1. One business day of system personnel notification of human resources (HR) action when accounts are no longer required;
    2. Immediately when users are terminated or transfer; and
    3. One week when system usage or need-to-know changes for an individual;
i. Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. Attributes required for authorizing access include restrictions on time of day, day of week, and point of origin as defined in Bureau or system Account Management Procedure;
j. Review accounts for compliance with account management requirements at least annually.
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.
m. Notifies account managers and sponsor, supervisor, COR, or other roles/personnel listed in Bureau or system account management procedures and on/off-boarding procedures:
    1. within one business day of system personnel notification of HR action when accounts are no longer required.
    2. immediately when users are terminated or transferred.
    3. within one week when system usage or need-to-know changes for an individual.
n. Authorize access to the system based on:
    1. A valid access authorization;
    2. Intended system usage; and
    3. to those approved by HR and their supervisors, to the systems and services connected to their daily obligations and position description based on groups with Active Directory.
o. Review accounts for compliance with account management requirements annually;
p. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
q. Align account management processes with personnel termination and transfer processes.

The [redacted] Account Management Guide and Access Control Compliance Procedures, version 1.4:

4.2.1.1
Privileged accounts are reviewed annually or more frequently as required depending on the addition of new users or removal to reflect changes in roles, responsibilities, or termination of employees.

4.6.5
[redacted] maintains a user log and change log for privileged and non-privileged accounts. The report is accessible from the Admin | Auditing | User Account Activity and Change Log reports.

To filter on user type or a specific user for example, the reports are exported as Microsoft (MS) Excel files where data filters are applied to query data for the intended purpose including auditing privileged account activity. User activity logs are audited on a weekly basis.

[redacted]:

[redacted] management did not identify the risk associated with not consistently performing reviews of [redacted] privileged user activity at a defined frequency and following up on any potential incidents.

A [redacted] administrator was not aware of the requirement to have all access requests and approvals documented within [redacted] prior to provisioning access.

[redacted]:

[redacted] [redacted] management performed a review of non-privileged users; however, lack of accountability over the re-authorization process led to the exclusion of privileged users within the listing used as the source for the review.

Due to competing priorities, [redacted] [redacted] management was delayed in the implementation of NIST 800-53, Revision 5, control updates and requirements and did not update the control frequency to review privileged user audit logs from annually to weekly.

[redacted]:

[redacted] management used an account management tool that did not properly identify the privileged user accounts that needed to be re-authorized for FY24. [redacted] management has a project in place to identify elevated access accounts that require re-authorization with a target date at the end of 2024.

[redacted]:

[redacted] management did not evaluate the risk associated with the lack of formal review of audit logs for [redacted] privileged users and follow up on any potential incidents.

[redacted] management informed us that due to the limited number of users with privileged access, it relied on verbal authorization of access.

[redacted]:

Due to the small size of [redacted], management did not evaluate the risk associated with the lack of defined and documented account management processes and procedures for [redacted].

[redacted] management prematurely closed a POA&M tracking the implementation of audit logging activities, via the Department Security Information and Event Management (SIEM) tool, to log activity on the [redacted] [redacted] which is the parent system for [redacted]. Specifically, [redacted] management was awaiting the Department's implementation of the SIEM project, which will enable monitoring and alerting on the activities of privileged users.

[redacted]:

[redacted] management did not evaluate the risk associated with the lack of formal review of audit logs for privileged-use activity.

[redacted]:

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

Failing to secure proper approval prior to the creation of privileged user account, there is an increased risk that inappropriate access may be granted. Additionally, management may not provision access or privileges that are commensurate with a users' job function or role. As a result, unauthorized access, disclosure, and/or modification of [redacted] production data and sensitive computing resources may occur.

[redacted]:

Without documentation to track the re-authorization of the privileged user accounts, there is an increased risk that inappropriate access is not identified and deactivated in a timely manner. As a result, unauthorized access, disclosure, and/or modification of [redacted] production data and sensitive computing resources may occur.

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

[redacted]:

Without sufficient controls in place to verify the completeness and accuracy of user populations used in management's periodic review of privileged [redacted] access, there is a risk that personnel retain access to privileged permissions that they no longer require. Such access could be used to compromise the confidentiality, integrity, or availability of [redacted] production data processed through the [redacted] systems.

[redacted]:

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

Without procedures in-place to document the authorization of privileged access of [redacted], there is an increased risk that inappropriate access may be granted and maintained. As a result, unauthorized access, disclosure, or modification of [redacted] production data and sensitive computing resources may occur.

[redacted]:

Without account management policies and procedures in-place, there is an increased risk that inappropriate access may be granted and maintained. Management may not remove [redacted] system access from terminated or transferred users in a timely manner. Additionally, management may not timely identify and adjust access or privileges that are no longer commensurate with a users' job function or role. As a result, unauthorized access, disclosure, and/or modification of [redacted] production data and sensitive computing resources may occur.

[redacted]:

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

We recommend [redacted]:

9. Formally document and implement procedures to review the audit logs of [redacted] privileged user activity in accordance with Interior security control standards.
10. Document evidence of the performed reviews with the reviewer's name and the date the review was performed. Evidence of the reviews should also include activities that were taken to investigate suspicious activity identified.
11. Ensure all [redacted] administrators with the responsibility of provisioning access are aware of the [redacted]

process and adhere to the approval process prior to granting any new or change of access roles.

We recommend [redacted]:

12. Ensure the list of users to be recertified is generated directly from the system and includes all privileged users.
13. Formally document the review and re-authorization of each user in accordance with Interior and [redacted] policies and procedures.
14. Implement privileged user activity audit log reviews for [redacted] users on a weekly basis in accordance with Interior and [redacted] policies and procedures.
15. Ensure the reviews are performed by an independent reviewer who does not have privileged roles to the system.

We recommend [redacted]:

16. Document procedures for performing the re-authorization of privileged [redacted] accounts in accordance with Interior policies.
17. Update the current re-authorization process and/configure the account management tool to ensure all user accounts are reviewed and re-authorized in accordance with Interior and [redacted] policies and procedures.

We recommend [redacted]:

18. Identify the events to be audited in accordance with AU-2 and the Interior Security and Privacy Control Standards for Audit and Accountability.
19. Formally document and implement procedures to review the audit logs of [redacted] privileged user activity in accordance with Interior security control standards.
20. Document evidence of the performed reviews with the reviewer's name and the date the review was performed. Evidence of the reviews should also include activities that were taken to investigate suspicious activity identified.
21. Document and maintain evidence of the approval of the privileged user access in accordance with the Interior Security and Privacy Control Standard.

We recommend [redacted]:

KPMG did not issue a recommendation due to the remediation activities identified in the condition.

We recommend [redacted]:

22. Document evidence of the performed review(s) with the reviewer's name and the date the review was performed.

4. Protect Function: Implementation of the ST Program.

The table below summarizes the deficiencies in the ST program.

FISMA Metric Domain	Summary of Deficiencies
ST	The Interior established a ST program; however, the Interior did not ensure that network access was removed for users that did not complete their annual RBST at [redacted].

We noted the following deficiency in the [redacted] ST program.

[redacted]:

Based on a selection of 25 users across the Department, we noted that [redacted] management did not remove network access for 1 of 2 [redacted] users that did not complete his/her annual RBST. Specifically, the RBST for this user was due on December 13, 2023 and, as of February 26, 2024, the user still had active network access and had not completed the training. The training was more than 75 days overdue. When [redacted] management was notified, they coordinated the user's completion of the RBST. [redacted] provided evidence that the training was complete as of March 12, 2024. Additionally, [redacted] provided evidence of the periodic review over training compliance. Specifically, [redacted] provided the report that is generated bi-monthly to review the training completion status of all [redacted] employees and the follow-up activity for those identified as non-compliant.

DOI Security and Privacy Control Standard – Awareness and Training (AT), AT-3 Role-Based Training, states

> Control:
> a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: significant information system, cybersecurity, or privacy responsibilities:
> 1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter; and
> 2. When required by system changes;
> b. Update role-based training content as needed following annual review and following when applicable laws, executive orders, directives, regulations, policies, standards, and guidelines change audit findings, incidents, or breaches; and
> c. Incorporate lessons learned from internal or external security or privacy incidents into role-based training.

Role-Based Security Training Standard, version 3.1, Section 4: DOI RBST, Non-Compliance and Reporting Non-Compliance:

> If a user does not complete RBST by the due date, they are non-compliant. Bureau and Office ACIOs are responsible for establishing procedures for disabling network access for non-compliant users' DOI network access no later than 14 days after the individual's certification expires as outlined in the Annual Training Directive and enforced by DM Part 370, Chapter 752. If extenuating circumstances are identified, an extension could be granted. An extension for those who temporarily cannot access the DOI network must not last longer than 60 days. All extensions must be documented and maintained as part of the bureaus' and offices' training compliance and completion record, which must be available to the OCIO and auditors upon request.

[redacted]:

[redacted] relies on the DOI Talent automated emails to notify the user and his/her supervisor of upcoming training. The user and the supervisor overlooked the reminder emails for the RBST requirement. Additionally, [redacted] does not review training compliance centrally on a periodic basis.

[redacted]:

Without completing RBST, a user may be more likely to inadvertently perform activities that may result in security and/or privacy incidents, including the unauthorized or inappropriate disclosure of sensitive data.

We recommend [redacted]:

KPMG did not issue a recommendation due to the remediation activities identified in the condition.

.

5. Detect Function: Implementation of the ISCM Program.

The table below summarizes deficiencies in the ISCM program.

FISMA Metric Domain	Summary of Deficiencies
ISCM	The Interior established an ISCM program; however, the Interior did not ensure that: • Program measures used to assess the effectiveness of its Interior ISCM program were defined to include the frequency of the collection and individuals responsible for the review. • The SSPP for one system was signed and approved by the system owner and designated authorizing officials at [redacted].

We noted the following deficiencies in the ISCM programs of the Interior and [redacted].

Interior:

The Interior did not fully identify, define and document the performance measures used to assess the effectiveness of its ISCM program for NIST SP 800-137 Tier 1, 2, and 3 to include the frequency of the collection and individual(s) responsible for the review.

[redacted]:

The Interior [redacted] SSPP was not signed and approved by the system owner, ISSO, and designated authorizing official to include the date of signature. Therefore, we were unable to determine whether system owner, ISSO, and designated authorizing official reviewed and approved the SSPP prior to the issuance of the Interior [redacted] Authority to Operate (ATO).

NIST SP 800-137, ISCM For Federal Information Systems and Organizations:

2.1.1 Tier 1-Organization - Tier 1 risk management activities address high-level information security governance policy as it relates to risk to the organization as a whole, to its core missions, and to its business functions. At this tier, the criteria for ISCM are defined by the organization's risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective. Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance. Tier 1 metrics are developed for supporting governance decisions regarding the organization, its core missions, and its business functions. Tier 1 metrics may be calculated based on security-related information from common, hybrid, and system-specific security controls. The metrics and the frequency with which they are monitored and reported are determined by requirements to maintain operations within organizational risk tolerances. As part of the overall governance structure established by the organization, the Tier 1 risk management strategy and the associated monitoring requirements are communicated throughout Tiers 2 and 3.

2.1.2 Tier 2 – Mission/Business Processes - Organizational officials that are accountable for one or more missions or business processes are also responsible for overseeing the associated risk management activities for those processes. The Tier 2 criteria for continuous monitoring of information security are defined by how core mission/business processes are prioritized with respect to the overall goals and objectives of the organization, the types of information needed to successfully execute the stated mission/business processes, and the organization-wide information

security program strategy. Controls in the Program Management (PM) family are an example of Tier 2 security controls. These controls address the establishment and management of the organization's information security program. Tier 2 controls are deployed organization-wide and support all information systems. They may be tracked at Tier 2 or Tier 1. The frequencies with which Tier 2 security controls are assessed and security status and other metrics are monitored are determined in part by the objectives and priorities of the mission or business process and measurement capabilities inherent in the infrastructure. Security-related information may come from common, hybrid, and system-specific controls. Metrics and dashboards can be useful at Tiers 1 and 2 in assessing, normalizing, communicating, and correlating monitoring activities below the mission/business processes tier in a meaningful manner.

2.1.3 Tier 3 – Information Systems - ISCM activities at Tier 3 address risk management from an information system perspective. These activities include ensuring that all system-level security controls (technical, operational, and management controls) are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time. ISCM activities at Tier 3 also include assessing and monitoring hybrid and common controls implemented at the system level. Security status reporting at this tier often includes but is not limited to security alerts, security incidents, and identified threat activities.17 The ISCM strategy for Tier 3 also ensures that security-related information supports the monitoring requirements of other organizational tiers. Data feeds/assessment results from system level controls (system-specific, hybrid, or common), along with associated security status reporting, support risk-based decisions at the organization and mission/business processes tiers. Information is tailored for each tier and delivered in ways that inform risk-based decision making at all tiers. Those resulting decisions impact the ISCM strategy applied at the information systems tier.

DOI OCIO Cybersecurity Division, *Enterprise ISCM Strategy*, *version 1*:

Section 4, Metrics and Measures:

The Cybersecurity Leadership Team (CSLT) holds responsibility for establishing and maintaining appropriate ISCM metrics for the enterprise in alignment with Federal and Departmental guidelines, policies, and standards, as well as in support of organization-specific business and mission priorities. This responsibility may be fulfilled via a designated working group. DOI bureaus/offices should leverage enterprise ISCM/Continuous Diagnostics and Mitigation (CDM) capabilities, metrics, and measures in reflecting the security posture of the bureau/office and enabling improved efficiencies. Additionally, the CIO is the primary responsible party for determining overall risk tolerance, but the AOs for each system have the ability to define and/or tailor risk tolerance for their specific system.

DOI Security and Privacy Control Standards Planning (PL), version 1.0, control PL-2 System Security and Privacy Plans:

a. Develop security and privacy plans for the system that:
    1. Are consistent with the organization's enterprise architecture;
    2. Explicitly define the constituent system components;
    3. Describe the operational context of the system in terms of mission and business processes;
    4. Identify the individuals that fulfill system roles and responsibilities;
    5. Identify the information types processed, stored, and transmitted by the system;
    6. Provide the security categorization of the system, including supporting rationale;
    7. Describe any specific threats to the system that are of concern to the organization;
    8. Provide the results of a privacy risk assessment for systems processing personally

identifiable information;

9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security and privacy requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security and privacy architecture and design decisions;
14. Include security- and privacy-related activities affecting the system that require planning and coordination with IT operations, DOI CIO and Privacy staff and at the bureau level between the ACIO, ACISO and/or SO; and
15. Are reviewed and approved by the AO or designated representative prior to plan implementation.

DOI Security and Privacy Control Standards Program Management (PM), version 4.1, control PM-10 Authorization Process:

a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
b. Designate individuals to fulfill specific roles and responsibilities within the DOI risk management process; and

NIST Special Publication 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems:

3.4 Authorizing Official - An authorizing official must be identified in the system security plan for each system. This person is the senior management official who has the authority to authorize operation (accredit) of an information system (major application or general support system) and accept the residual risk associated with the system. The assignment of the authorizing official should be in writing, and the plan must include the same contact information listed in Section 3.3.

3.15 Completion and Approval Dates - The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. When the system is updated, a version number should be added. The system security plan should also contain the date the authorizing official or the designated approving authority approved the plan. Approval documentation, i.e., accreditation letter, approval memorandum, should be on file or attached as part of the plan.

Interior:

Due to competing priorities and new directives from the federal government and the Department, the Interior ISCM program was not given the focus to ensure performance measures were identified, defined and documented.

[redacted]:

[redacted] management failed to identify the risk associated with the lack of approval and signature of the Interior [redacted] SSPP.

Interior:

Without an effective continuous monitoring strategy to collect and monitor performance metrics, management is at risk of not having awareness of the security and privacy posture. As a result, management is unable to make effective and timely risk-based decisions to support their goals and mission statements.

[redacted]:

Without the review and approval of the SSPP by the authorizing official, there could be underlying residual risks associated with the system that have not been accepted, which increases the risk that the system is operating without appropriate controls to protect the system's confidentiality, integrity, and availability.

We recommend the Interior:

23. Identify, define, and document the performance measures and requirements that will be used to assess the effectiveness of its ISCM program for Tier 1, 2, and 3, as appropriate.
24. Define and document the frequency of the collection of the performance measures and the individuals responsible for the review of the metrics.

We recommend [redacted], [redacted] authorizing official, system owner, and ISSO:

25. Update, review, and approve the [redacted] SSPP. Additionally, the [redacted] should establish a quality control process to remind the ISSO, system owner, and designated authorizing official to review, update, and approve the SSPP in accordance with Interior policy and NIST security requirements.

6. Respond Function: Implementation of the IR Program.

The table below summarizes the deficiencies in the IR program.

FISMA Metric Domain	Summary of Deficiencies
IR	The Interior established an IR program; however, the Interior did not operate the Event Logging (EL) and retention program at the [redacted] maturity tier and the [redacted] maturity tier for the Department.

We noted the following deficiency at in the IR program at the Interior.

Interior:

The Interior event log management and retention program was operating at the [redacted] maturity, defined as logging requirements of highest criticality are only partially met. The Interior did not fully implement the event logging and retention requirements specified within the OMB Memorandum M-21-31 and is not able to specifically evidence the achievement of [redacted] and [redacted] requirements.

OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents:

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.

[redacted]

[redacted]

Interior:

> The Interior Office of the [redacted] management informed us that the [redacted] and [redacted] requirements require extensive human and technological resources and that the current capabilities are limited.

Interior:

> Lack of effective logging requirements increases the risk that the Interior and the Federal Government is not able to utilize the information from logs on Interior systems to detect, investigate, and remediate cyber threats impacting the system's confidentiality, integrity, and availability.

We recommend the Interior:

26. Acquire the capabilities and allocate resources to effectively implement the requirements outlined in OMB M-21-31 for [redacted] and [redacted].
27. Enhance event log management policies and procedures to aid in the implementation of the requirements outlined in OMB M-21-31.

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 IG FISMA Reporting Metrics. We identified control deficiencies associated with the following FISMA Metric Domains: SCRM, CM, IAM, ST, ISCM, and IR.

Based on the IG FISMA Reporting Metrics guidance and on the CyberScope results, the Interior's information security program was assessed as not effective because the calculated average of the Cybersecurity Functions was assessed at Consistently Implemented (Level 3).

We made 27 recommendations related to the control deficiencies we identified during the FISMA performance audit. If effectively implemented by management, these remediations should strengthen the Interior's information security program.

The root causes that led to the control deficiencies identified as part of this performance audit may contribute to or be reflective of 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, the Interior 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, the Interior concurred with our recommendations and, where appropriate, provided planned corrective actions that were responsive to the intent of our recommendations (see next section).

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

November 22, 2024

Memorandum

To: Mark Lee Greenblatt
Inspector General

Through: Darren B. Ash
DARREN ASH Digitally signed by DARREN ASH Date: 2024.11.22 16:25:35 -05'00'
Chief Information Officer
Office of the Chief Information Officer

From: Stanley F. Lowe
Digitally signed by STANLEY LOWE Date: 2024.11.22 14:37:50 -05'00'
Chief Information Security Officer
Office of the Chief Information Officer

Subject: Response to Office of Inspector General Draft Fiscal Year 2024 FISMA Report by Independent Public Auditor (2024-CTD-006)

Thank you for providing the Department of the Interior (Department, Interior) the Office of Inspector General (OIG) Draft Report on October 23, 2024 of the *Federal Information Security Modernization Act of 2014 Fiscal Year 2024 Performance Audit (2024–CTD–006).* 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: Sherrill Exum, Chief, Audit Management Division, Office of Financial Management
Information Management and Technology Leadership Team
Cybersecurity Leadership Team
Richard Westmark, Chief, Compliance Management Section, Office of the Chief Information Officer

Attachment 1: FISMA Recommendations and Interior Responses (2024-CTD-006)

1. **Interior: Develop and implement enterprise-wide policies and procedures to detect and prevent counterfeit components from entering the environment.**

   Concur. The Interior Office of the Chief Information Officer (OCIO), together with bureau and office information management technology (IMT) leadership, will review and update Interior's Enterprise Cybersecurity Supply Chain Risk Management (C-SCRM) policies and guidance to ensure that prevention, detection, and training related to anti-counterfeit/component authenticity are properly addressed. In addition, Interior will develop and provide anti-counterfeit/component authenticity training for designated personnel.

   Plan of Actions and Milestones (POA&Ms) ID: Enterprise Cybersecurity Program (ECP) POA&M [redacted]; Target date: [redacted]
   Responsible Official: Stanley Lowe, Chief Information Security Officer (CISO)

2. **Interior: Develop and provide component authenticity and anti-counterfeit training to all designated personnel at least annually or at a frequency defined by Interior.**

   Concur. The Interior OCIO together with bureau and office IMT leadership will review and update Interior's Enterprise C-SCRM policies and guidance to ensure that prevention, detection, and training related to anti-counterfeit/component authenticity are properly addressed. In addition, Interior will develop and provide anti-counterfeit/component authenticity training for designated personnel.

   POA&M ID: ECP POA&M [redacted]; Target date: [redacted]
   Responsible Official: Stanley Lowe, CISO

3. **Interior: Oversee Bureaus and Offices to make sure that they implement their own SCRM policies and procedures respective to their unique risks in a documented and approved plan, which will be structured based on the Interior SCRM Strategy.**

   Concur. The Interior OCIO together with bureau and office IMT leadership will work to continue implementation of Interior's Enterprise C-SCRM Program. Implementation includes ensuring that all bureaus/offices have approved C-SCRM plans that align with the Interior Enterprise C-SCRM Strategy V2 as well as appropriate timelines. Interior will also work to complete implementation of processes to review and assess supply chain related risks through evaluation of established supply chain controls for information technology (IT) systems and services across the Department. In addition, Interior will develop and implement performance metrics to ensure compliance with agency C-SCRM policies and standards.

   POA&M ID: ECP POA&M [redacted]; Target date: [redacted]
   Responsible Official: Stanley Lowe, CISO

4. **Interior: Implement a process to consistently assess and review the supply chain-related risks through evaluation that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet applicable regulations across all bureaus and offices.**

   Concur. The Interior OCIO together with bureau and office IMT leadership will work to continue implementation of Interior's Enterprise C-SCRM Program. Implementation includes ensuring that all bureaus and offices have approved C-SCRM plans that align with the Interior Enterprise C-SCRM Strategy V2 as well as appropriate timelines. Interior will also work to complete implementation of processes to review and assess supply chain related risks through evaluation of established supply chain controls for IT systems and services across the Department. In addition, Interior will develop

and implement performance metrics to ensure compliance with agency C-SCRM policies and standards.

POA&M ID: ECP POA&M [redacted]; Target date: [redacted]
Responsible Official: Stanley Lowe, CISO

5. **Interior: Develop and implement a Department-level monitoring and enforcing process to ensure compliance with the overall SCRM program policies.**

   Concur. The Interior OCIO together with bureau and office IMT leadership will work to continue implementation of Interior's Enterprise C-SCRM Program. Implementation includes ensuring that all bureaus and offices have approved C-SCRM plans that align with the Interior Enterprise C-SCRM Strategy V2 as well as appropriate timelines. Interior will also work to complete implementation of processes to review and assess supply chain-related risks through evaluation of established supply chain controls for IT systems and services across the Department. In addition, Interior will develop and implement performance metrics to ensure compliance with agency C-SCRM policies and standards.

   POA&M ID: ECP POA&M [redacted]; Target date: [redacted]
   Responsible Official: Stanley Lowe, CISO

6. **[redacted]: Remediate [redacted] vulnerabilities on the [redacted] system in accordance with the timeframes established in applicable Interior Security Control Standards and [redacted] policies.**

   Concur. [redacted] will investigate the identified vulnerabilities and remediate them within the timelines established by Interior and [redacted] policy or document risk-based decisions as appropriate. To track this effort, the [redacted] has established POA&M # [redacted] System And Information Integrity (SI)-2: Flaw Remediation instead of [redacted], as the servers with these vulnerabilities are part of the [redacted] security boundary.

   POA&M ID# [redacted]; Target date: [redacted]
   Responsible Official: [redacted] Associate Chief Information Officer (ACIO)

7. **[redacted]: Implement an oversight process that provides accountability for system owners to remediate vulnerabilities timely or obtain risk acceptances, as appropriate.**

   Concur. The [redacted] will review vulnerability remediation procedures and validate that accountability for remediation or documentation of risk-based decisions are monitored via the Bison Governance, Risk, and Compliance (GRC) tool. To track this effort, the [redacted] has established POA&M # [redacted] Cybersecurity and Privacy Program (CSPP) SI-2: Flaw Remediation - Lack of Flaw Remediation Oversight.

   POA&M ID# [redacted]; Target date: [redacted]
   Responsible Official: [redacted] ACIO

8. **[redacted]: Improve the implementation for all configuration changes to make control owners formally aware of the process and abide by the required change process workflow based on the type of change. [redacted] management should review the change made to the [redacted] environment in FY 2024 to confirm that it did not have an adverse impact on [redacted] functionality.**

Concur. The [redacted] will review the change made to the [redacted] environment in Fiscal Year (FY) 2024 and confirm that it did not have an adverse impact on [redacted] functionality in accordance with the [redacted] configuration management plan procedures. Additionally, the [redacted] will update the system's configuration management plan to require all changes, regardless of type, to be documented via the Bison Support System and abide by the appropriate process workflow. To track this effort, the [redacted] has established POA&M # [redacted] Continuous Monitoring (CM)-3(2): Failed Testing, Validation, and Documentation of Changes.

POA&M ID# [redacted]; Target date: [redacted]
Responsible Official: [redacted] ACIO

9. [redacted]: Formally document and implement procedures to review the audit logs of [redacted] privileged user activity in accordance with Interior security control standards.

Concur. [redacted] will formally document and implement procedures to review [redacted] audit logs of privileged user activity in accordance with the Interior security control standards.

POA&M ID# [redacted]; Target date: [redacted]
Responsible Official: [redacted] ACIO

10. [redacted]: Document evidence of the performed reviews with the reviewer's name and the date the review was performed. Evidence of the reviews should also include activities that were taken to investigate suspicious activity identified.

Concur. [redacted] will document evidence of the performed reviews with the reviewer's name, the date the review was performed, and activities that were taken to investigate identified suspicious activities.

POA&M ID# [redacted]; Target date: [redacted]
Responsible Official: [redacted] ACIO

11. [redacted]: Ensure all [redacted] administrators with the responsibility of provisioning access are aware of the [redacted] process and adhere to the approval process prior to granting any new or change of access roles.

Concur. [redacted] will implement a process to ensure [redacted] administrators with responsibility of provisioning access are aware of the [redacted] process and adhere to the approval process prior to granting any new or change of access roles.

POA&M ID# [redacted]; Target date: [redacted]
Responsible Official: [redacted] ACIO

12. [redacted]: Ensure the list of users to be recertified is generated directly from the system and includes all privileged users.

Concur. [redacted] will implement processes and procedures for annual review and re-authorization of all [redacted] users, including privileged users. These will include generating a list of all [redacted] users, exported from the application, to be followed by review and re-authorization of the users by the System Owner and Contracting Officer's Representative (COR). The document will be electronically signed and saved within the system. Based on outcomes of the review and re-authorization process, required changes to user accounts will be made by the systems administrator. Implemented [redacted].

POA&M ID: [redacted] *POA&M* [redacted]*; Target date:* [redacted]
Responsible Official: [redacted]

13. [redacted]**: Formally document the review and re-authorization of each user in accordance with Interior and** [redacted] **policies and procedures.**

Concur. [redacted] *will implement processes and procedures for annual review and re-authorization of all* [redacted] *users, including privileged users. These will include generating a list of all* [redacted] *users, exported from the application, to be followed by review and re-authorization of the users by the System Owner and COR. The document will be electronically signed and saved within the system. Based on outcomes of the review and re-authorization process, required changes to user accounts will be made by the systems administrator. Implemented* [redacted].

POAM ID: [redacted] *POAM* [redacted]*; Target date:* [redacted]
Responsible Official: [redacted]

14. [redacted]**: Implement privileged user activity audit log reviews for** [redacted] **users on a weekly basis, in accordance with Interior and** [redacted] **policies and procedures.**

Concur. [redacted] *will implement processes and procedures to ensure privileged user activity audit log reviews are performed by an independent reviewer, who does not have any privileged roles in the system. Results of the review by the independent reviewer will be electronically signed and stored in the system. Implemented* [redacted].

POAM ID: [redacted] *POAM* [redacted]*; Target date:* [redacted]
Responsible Official: [redacted]

15. [redacted]**: Ensure the reviews are performed by an independent reviewer, who does not have privileged roles to the system.**

Concur. [redacted] *will implement processes and procedures to ensure privileged user activity audit log reviews are performed by an independent reviewer who does not have any privileged roles in the system. Results of the review by the independent reviewer will be electronically signed and stored in the system. Implemented* [redacted].

POAM ID: [redacted] *POAM* [redacted]*; Target date:* [redacted]
Responsible Official: [redacted]

16. [redacted]**: Document procedures for performing the re-authorization of privileged** [redacted] **accounts in accordance with Interior policies.**

Concur. [redacted] *will document standard operating procedures (SOP) for re-authorization of privileged accounts. The SOP will address re-authorization of all privileged accounts, including accounts under* [redacted].

POAM ID: [redacted] *#* [redacted] *(*[redacted]*);*
Target date: [redacted]
Responsible Official: [redacted] *Associate CISO (ACISO)*

17. [redacted]**: Update the current re-authorization process and/configure the account management tool to ensure all user accounts are reviewed and re-authorized in accordance with Interior and** [redacted] **policies and procedures.**

Concur.

- *Immediate: Perform immediate review of existing Elevated Privilege accounts and notify users who have not recertified within the last 365 days. We have disabled accounts if they did not recertify by* [redacted].
- *Short term:* [redacted] *will also perform a quarterly review of existing elevated accounts for suitability until the new elevated account process is implemented.*
- *Longer Term:* [redacted] *will re-architect the current privileged re-authorization process. This will allow us to complete an alternative analysis review to identify the appropriate account management tool.*

POAM ID: [redacted] *#*[redacted]*);*
Target date: [redacted]
Responsible Official: [redacted] *ACISO*

18. [redacted]**: Identify the events to be audited in accordance with AU-2 and the Interior Security and Privacy Control Standards for Audit and Accountability.**

Concur. The [redacted] *system boundary has taken immediate actions to improve its review of audit logs for privileged users. POA&M #*[redacted] *was created to formally design and implement procedures to review* [redacted] *system audit logs of privileged user activity in accordance with Interior Standards.*

POA&M ID #[redacted]*; Target date:* [redacted]
Responsible Official: [redacted] *ACISO*

19. [redacted]**: Formally document and implement procedures to review the audit logs of** [redacted] **privileged user activity in accordance with Interior security control standards.**

Concur. The [redacted] *system boundary has taken immediate actions to improve its review of audit logs for privileged users. Plan of Action and Milestones (POAM) #*[redacted] *was created to formally design and implement procedures to review* [redacted] *system audit logs of privileged user activity in accordance with Interior Standards.*

POA&M ID#[redacted]*; Target date:* [redacted]
Responsible Official: [redacted] *ACISO*

20. [redacted]**: Document evidence of the performed reviews with the reviewer's name and the date the review was performed. Evidence of the reviews should also include activities that were taken to investigate suspicious activity identified.**

Concur. The [redacted] *system boundary has taken immediate actions to improve its review of audit logs for privileged users. POA&M #*[redacted] *was created to formally design and implement procedures to review* [redacted] *system audit logs of privileged user activity in accordance with Interior standards.*

POA&M ID#[redacted]*; Target date:* [redacted]
Responsible Official: [redacted] *ACISO*

21. [redacted]**: Document and maintain evidence of the approval of the privileged user access, in accordance with the Interior Security and Privacy Control Standard.**

Concur. The [redacted] *system boundary has taken immediate actions to improve its review and reauthorize privileged users. POA&M #*[redacted] *has been created to initiate the design and implementation*

of procedures to review and reauthorize privileged [redacted] user access annually in accordance with the Interior standards. The process will document and maintain evidence of the completion of the privileged user access review and reauthorization.

POA&M ID#[redacted]; Target date:[redacted]
Responsible Official:[redacted] ACISO

22. [redacted]: Document evidence of the performed review(s) with the reviewer's name and the date the review was performed.

Concur.[redacted] has completed actions to comply with this requirement. Audit log reviewers document weekly log reviews to show the reviewer's name and date the review was performed. In addition,[redacted] local standard operating procedures have been updated to include this requirement. Implemented[redacted].

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

23. Interior: Identify, define, and document the performance measures and requirements that will be used to assess the effectiveness of its ISCM program for Tier 1, 2, and 3, as appropriate.

Concur. The Interior OCIO together with bureau and office IMT leadership will update Interior's Enterprise Information Security Continuous Monitoring (ISCM) Strategy to define and document performance measures to assess the effectiveness of the Interior ISCM program. This includes documenting the frequency of metrics collection and identifying roles and responsibilities related to the on-going review of ISCM Program performance metrics.

POA&M ID:[redacted] POA&M[redacted]; Target date:[redacted]
Responsible Official: Stanley Lowe, CISO

24. Interior: Define and document the frequency of the collection of the performance measures and the individuals responsible for the review of the metrics.

Concur. The Interior OCIO together with bureau and office IMT leadership will update Interior's Enterprise ISCM Strategy to define and document performance measures to assess the effectiveness of the Interior ISCM program. This includes documenting the frequency of metrics collection and identifying roles and responsibilities related to the on-going review of ISCM Program performance metrics.

POA&M ID:[redacted] POA&M[redacted]; Target date:[redacted]
Responsible Official: Stanley Lowe, CISO

25. [redacted]: [redacted], [redacted] authorizing official, system owner, and ISSO update, review, and approve the [redacted] SSPP. Additionally, the [redacted] should establish a quality control process to remind the ISSO, system owner, and designated authorizing official to review, update, and approve the SSPP in accordance with the Interior policy and NIST security requirements.

Concur.[redacted] concurs that the required approvers, as defined by the National Institute of Standards and Technology (NIST), must formally approve the System Security and Privacy Plans (SSPPs) for all information systems prior to issuing an ATO. To facilitate this process, the workflow in the GRC system will be updated to ensure this step is built into the overall process.

POA&M ID#[redacted]; Target date:[redacted]
Responsible Official:[redacted]

26. Interior: Acquire the capabilities and allocate resources to effectively implement the requirements outlined in OMB M-21-31 for[redacted] and[redacted].

Concur. The Department will continue to request funding to acquire resources to implement logging requirements and plan project implementation once resources are provided.

POA&M ID:[redacted] POA&M[redacted]; Target date:[redacted]
Responsible Official:[redacted]

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

Concur.[redacted] Cybersecurity engineering team will develop model policies and procedures to aid in the implementation of the logging requirements within current resources.

POA&M ID:[redacted] POA&M[redacted]; Target date:[redacted]
Responsible Official:[redacted]

List 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
APO	Associate Privacy Officers
[redacted]	[redacted]
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
A&A	Assessment and Authorization
BIA	Bureau of Indian Affairs
BisonGRC	Bison Governance, Risk and Compliance
BLM	Bureau of Land Management
BOEM [redacted]	Bureau of Ocean Energy Management [redacted]
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
BSS	Bison System Support
CDM	Continuous Diagnostics and Mitigation
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
COR	Contracting Officer's Representative
CP	Contingency Planning
CSIRT	Computer Security Incident Response Team
CSLT	Cybersecurity Leadership Team
C-SCRM	Cybersecurity Supply Chain Risk Management
DHS	Department of Homeland Security
DOI	Department of the Interior
DNS	Domain Name Service
DPO	Departmental Privacy Officer
DP&P	Data Protection and Privacy
[redacted]	[redacted]
ECRM	Enterprise Cybersecurity Risk Management
EDR	Endpoint Detection Response
EL	Event Logging
EO	Executive Order
FBI	Federal Bureau of Investigations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
[redacted]	[redacted]
FWS	US Fish and Wildlife Service
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
HR	Human Resource

Acronym	Definition
HVA	High Value Asset
IA	Information Assurance
IAM	Identity and Access Management
IBC	Interior Business Center
ICT	Information & Communications Technology
IG	Inspector General
IMT	Interior Information Management and Technology
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
[redacted]	[redacted]
[redacted]	[redacted]
MFA	Multifactor Authentication
MS	Microsoft
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
[redacted]	[redacted]
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OFCIO	Office of the Federal Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSMRE	Office of Surface Mining Reclamation and Enforcement

Acronym	Definition
PIV	Personal Identity Verification
PL	Planning
POA&M	Plan of Action and Milestones
PM	Program Management
RA	Risk Assessment
[redacted]	[redacted]
RBST	Role-Based Security Training
REV	Revision
RM	Risk Management
RMO	Resource Management Office
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
SCS	Security Control Standard
SI	System and Information Integrity
SIEM	Security Information and Event Management
SO	System Owner
SOL	Office of the Solicitor
SOP	Standard Operating Procedure
SP	Special Publication
SR	Supply Chain Risk Management
SSPP	System Security and Privacy Plan
ST	Security Training
[redacted]	[redacted]
US	United States
USGS	United States Geological Survey
[redacted]	[redacted]

Appendix I – Summary of Program Areas Bureaus and Offices That 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 IV or responses provided for the FY 2024 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.

Cybersecurity Function Deficiencies Identified by Organization

Functions	Interior	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Identify	X											
Protect			X	X	X	X		X	X			X
Detect	X									X		
Respond	X											
Recover												

Appendix II – Status of 2023 Recommendations

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 FY23 FISMA report recommendations and their respective statuses as of August 23, 2024.

Recommendation Description	Status Open/Closed and Target Completion Date
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 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.	Closed 3/7/2024
2. [redacted]: Enhance the POA&M maintenance process to ensure that all bureau-level open POA&Ms are reviewed and updated quarterly in accordance with Interior policy.	Closed 5/3/2024
2. [redacted]: Enhance the POA&M maintenance process to ensure that all bureau-level open POA&Ms are reviewed and updated quarterly in accordance with Interior policy.	[redacted]
2. [redacted]: Enhance the POA&M maintenance process to ensure that all bureau-level open POA&Ms are reviewed and updated quarterly in accordance with Interior policy.	Closed 7/24/2024
2. [redacted]: Enhance the POA&M maintenance process to ensure that all bureau-level open POA&Ms are reviewed and updated quarterly in accordance with Interior policy.	Closed 6/25/2024
3. [redacted]: Ensure all required fields such as milestone and scheduled completion dates are documented and defined for each open POA&M.	Closed 5/3/2024
3. [redacted]: Ensure all required fields such as milestone and scheduled completion dates are documented and defined for each open POA&M.	[redacted]
3. [redacted]: Ensure all required fields such as milestone and scheduled completion dates are documented and defined for each open POA&M.	Closed 7/24/2024
3. [redacted]: Ensure all required fields such as milestone and scheduled completion dates are documented and defined for each open POA&M.	Closed 6/13/2024
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.	[redacted]

Recommendation Description	Status Open/Closed and Target Completion Date
5. [redacted]: Design and implement policies and procedures for the baseline configuration reviews of [redacted] and [redacted].	[redacted]
6. [redacted]: Maintain evidence of [redacted] and [redacted] baseline configuration review and compliance with established baselines.	[redacted]
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.	Closed 5/16/2024
8. [redacted]: Update configuration management related policies and procedures to include the process for the review of [redacted] [redacted] system baseline configuration compliance checks.	Closed 5/13/2024
9. [redacted]: Ensure [redacted] management conduct the review of baseline configuration compliance checks and maintain evidence of review.	Closed 6/5/2024
10. [redacted]: Ensure all critical and high-risk vulnerabilities in the [redacted] environment are remediated in accordance with the timeframes established in the Interior 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.	Closed 6/11/2024
11. [redacted]: Design and implement a process to periodically review the [redacted] system baseline security configuration for compliance.	Closed 5/23/2024
12. [redacted]: Design and implement a process to review vulnerability scans in accordance with Interior SCS. Implement a mechanism to enforce the requirements outlined in the Interior RA and SI SCS for the [redacted] system.	Closed 5/21/2024
13. Implement a mechanism to enforce the requirements outlines in the Interior RA and SI SCS for the [redacted] system.	Closed 5/14/2024
14. [redacted]: Develop and implement corrective actions related to the [redacted] POA&Ms for the following four vulnerabilities: [redacted]	Closed 7/24/2024
15. [redacted]: Implement a mechanism to enforce the requirements outlined in the Interior RA and SI SCS for the [redacted] system.	Closed 7/24/2024

Recommendation Description	Status Open/Closed and Target Completion Date
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 the Interior SCS.	[redacted]
17. [redacted]: Design and implement [redacted] policies and procedures for privileged users to ensure users with access to the development environment do not also have access to the production environment.	[redacted]
18. [redacted]: Design and implement policies and procedures to perform independent audit log reviews for all [redacted] privileged user activities in accordance with the Interior SCS.	[redacted]
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.	[redacted]
20. [redacted]: Implement procedures to review the audit logs of system administrator activity in accordance with the Interior SCS and the [redacted] policies and procedures.	[redacted]
21. [redacted]: Identify an audit log reviewer that is independent of the privileged users' activities noted in the audit logs.	[redacted]
22. [redacted]: Maintain evidence of privileged user activity reviews performed for the [redacted] to include the reviewer's name and the date the review was performed.	[redacted]
23. [redacted]: Design and implement procedures to review and reauthorize privileged [redacted] system users access annually in accordance with the Interior SCS.	Closed 4/25/2024
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.	Closed 2/8/2024
25. The Interior CIRC and Bureau/Office Security Analysts: Implement a process to ensure that the Interior CIRC analysts are trained to perform activities in alignment with the one-hour reporting requirement in accordance with the Interior SCS.	Closed 7/8/2024

Recommendation Description	Status Open/Closed and Target Completion Date
26. Interior: Acquire the data storage needed to effectively implement the data retention requirements outlined in OMB M-21-31.	[redacted]
27. Interior: Enhance event log management policies and procedures to aid in the implementation of the requirements outlined in OMB M-21-31.	[redacted]
28. Interior: Establish a monitoring process to ensure all Bureaus and Offices have effectively implemented the revised event log management policies and procedures.	[redacted]
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.	Closed 5/15/2024

Appendix III – NIST SP 800-53 Rev. 5.1.1 Security Control Considerations

The table below represents the Cybersecurity Functions 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. 5.1.1: CA-3	System Interconnections
NIST SP 800-53, Rev. 5.1.1: CA-7	Continuous Monitoring
NIST SP 800-53, Rev. 5.1.1: CM-8	Information System Component Inventory
NIST SP 800-53, Rev. 5.1.1: CM-10	Software Usage Restrictions
NIST SP 800-53, Rev. 5.1.1: CM-11	User-Installed Software
NIST SP 800-53, Rev. 5.1.1: PL-8	Information Security Architecture
NIST SP 800-53, Rev. 5.1.1: PM-5	Information System Inventory
NIST SP 800-53, Rev. 5.1.1: PM-7	Enterprise Architecture
NIST SP 800-53, Rev. 5.1.1: PM-9	RM Strategy
NIST SP 800-53, Rev. 5.1.1: PM-11	Mission/Business Process Definition
NIST SP 800-53, Rev. 5.1.1: RA-2	Security Categorization
NIST SP 800-53, Rev. 5.1.1: RA-3	Risk Assessment
NIST SP 800-53, Rev. 5.1.1: SA-3	System Development Life Cycle
NIST SP 800-53, Rev. 5.1.1: SA-8	Security Engineering Principles
NIST SP 800-53, Rev. 5.1.1: SA-9	External System Services
NIST SP 800-53, Rev. 5.1.1: SA-12	Supply Chain Protection
Cybersecurity Identify Function: SCRM	
NIST SP 800-53, Rev. 5.1.1: SA-4	Acquisition Process
NIST SP 800-53, Rev. 5.1.1: SR-3	Supply Chain Controls and Processes
NIST SP 800-53, Rev. 5.1.1: SR-5	Acquisition Strategies, Tools, and Methods
NIST SP 800-53, Rev. 5.1.1: SR-6	Supplier Assessments and Reviews
NIST SP 800-53, Rev. 5.1.1: SR-11	Component Authenticity
Cybersecurity Protect Function: CM	
NIST SP 800-53, Rev. 5.1.1: CM-1	CM Policy and Procedures
NIST SP 800-53, Rev. 5.1.1: CM-2	Baseline Configuration
NIST SP 800-53, Rev. 5.1.1: CM-3	Configuration Change Control
NIST SP 800-53, Rev. 5.1.1: CM-4	Impact Analyses
NIST SP 800-53, Rev. 5.1.1: CM-6	Configuration Settings
NIST SP 800-53, Rev. 5.1.1: CM-7	Least Functionality
NIST SP 800-53, Rev. 5.1.1: CM-8	Information System Component Inventory
NIST SP 800-53, Rev. 5.1.1: CM-9	CM Plan
NIST SP 800-53, Rev. 5.1.1: RA-5	Vulnerability Monitoring and Scanning
NIST SP 800-53, Rev. 5.1.1: SI-2	Flaw Remediation
NIST SP 800-53, Rev. 5.1.1: SI-3	Malicious Code Protection
Cybersecurity Protect Function: IAM	
NIST SP 800-53, Rev. 5.1.1: AC-1	AC Policy and Procedures
NIST SP 800-53, Rev. 5.1.1: AC-2	Account Management
NIST SP 800-53, Rev. 5.1.1: AC-5	Separation of Duties
NIST SP 800-53, Rev. 5.1.1: AC-6	Least Privilege
NIST SP 800-53, Rev. 5.1.1: AC-8	System Use Notification
NIST SP 800-53, Rev. 5.1.1: AC-17	Remote Access

NIST SP 800-53, Rev. 5.1.1: AU-2	Audit Logging
NIST SP 800-53, Rev. 5.1.1: AU-3	Content of Audit Records
NIST SP 800-53, Rev. 5.1.1: AU-6	Audit Record Review, Analysis, and Reporting
NIST SP 800-53, Rev. 5.1.1: IA-1	IA Policy and Procedures
NIST SP 800-53, Rev. 5.1.1: IA-2	Identification and Authentication
NIST SP 800-53, Rev. 5.1.1: IA-4	Identifier Management
NIST SP 800-53, Rev. 5.1.1: IA-5	Authenticator Management
NIST SP 800-53, Rev. 5.1.1: PE-3	Physical Access Control
NIST SP 800-53, Rev. 5.1.1: PS-1	Personnel Security Policy and Procedures
NIST SP 800-53, Rev. 5.1.1: PS-2	Position Risk Determination
NIST SP 800-53, Rev. 5.1.1: PS-3	Personnel Screening
NIST SP 800-53, Rev. 5.1.1: PS-6	Access Agreements
Cybersecurit Protect Function: DP&P	
NIST SP 800-53, Rev. 5.1.1: AT-1	Policies and Procedures
NIST SP 800-53, Rev. 5.1.1: AT-2	Literacy Training and Awareness
NIST SP 800-53, Rev. 5.1.1: AT-3	Role-Based Training
NIST SP 800-53, Rev. 5.1.1: IR-8	Incident Response Plan
NIST SP 800-53, Rev. 5.1.1: MP-3	Media Marking
NIST SP 800-53, Rev. 5.1.1: MP-6	Media Sanitization
NIST SP 800-53, Rev. 5.1.1: PL-4	Rules of Behavior
NIST SP 800-53, Rev. 5.1.1: SC-7	Boundary Protection
NIST SP 800-53, Rev. 5.1.1: SC-8	Transmission Confidentiality and Integrity
NIST SP 800-53, Rev. 5.1.1: SC-18	Mobile Code
NIST SP 800-53, Rev. 5.1.1: SC-28	Protection of Information at Rest
NIST SP 800-53, Rev. 5.1.1: SI-3	Malicious Code Protection
NIST SP 800-53, Rev. 5.1.1: SI-4	Information System Monitoring
NIST SP 800-53, Rev. 5.1.1: SI-7	Software, Firmware, and Information Integrity
NIST SP 800-53, Rev. 5.1.1: SI-12	Boundary Protection
Cybersecurity Protect Function: ST	
NIST SP 800-53, Rev. 5.1.1: AT-1	Security Awareness and Training Policy and Procedures
NIST SP 800-53, Rev. 5.1.1: AT-2	Security Awareness Training
NIST SP 800-53, Rev. 5.1.1: AT-3	Role-Based Security Training
NIST SP 800-53, Rev. 5.1.1: AT-4	Security Training Records
NIST SP 800-53, Rev. 5.1.1: PM-13	Security and Privacy Workforce
Cybersecurity Detect Function: ISCM	
NIST SP 800-53, Rev. 5.1.1: CA-2	Security Assessments
NIST SP 800-53, Rev. 5.1.1: CA-5	Plan of Action and Milestones
NIST SP 800-53, Rev. 5.1.1: CA-6	Security Authorization
NIST SP 800-53, Rev. 5.1.1: CA-7	Continuous Monitoring
NIST SP 800-53, Rev. 5.1.1: PL-2	System Security and Privacy Plans
NIST SP 800-53, Rev. 5.1.1: PM-6	Measures of Performance
NIST SP 800-53, Rev. 5.1.1: PM-10	Authorization Process
NIST SP 800-53, Rev. 5.1.1: PM-14	Testing, Training, and Monitoring
NIST SP 800-53, Rev. 5.1.1: PM-31	Continuous Monitoring Strategy
Cybersecurity Respond Function: IR	
NIST SP 800-53, Rev. 5.1.1: IR-4	Incident Handling
NIST SP 800-53, Rev. 5.1.1: IR-5	Incident Monitoring
NIST SP 800-53, Rev. 5.1.1: IR-6	Incident Reporting
NIST SP 800-53, Rev. 5.1.1: IR-7	Incident Response Assistance

NIST SP 800-53, Rev. 5.1.1: IR-8	Incident Response Plan
Cybersecurity Recover Function: CP	
NIST SP 800-53, Rev. 5.1.1: CP-2	CP Plan
NIST SP 800-53, Rev. 5.1.1: CP-3	CP Training
NIST SP 800-53, Rev. 5.1.1: CP-4	CP Testing
NIST SP 800-53, Rev. 5.1.1: CP-6	Alternate Storage Site
NIST SP 800-53, Rev. 5.1.1: CP-7	Alternate Processing Site
NIST SP 800-53, Rev. 5.1.1: CP-8	Telecommunications Services
NIST SP 800-53, Rev. 5.1.1: CP-9	Information System Backup
NIST SP 800-53, Rev. 5.1.1: CP-10	System Recovery and Reconstitution
NIST SP 800-53, Rev. 5.1.1: RA-9	Criticality Analysis

Appendix IV – 2024 Maturity Levels for the IG FISMA Reporting Metrics

This appendix describes the assessed maturity levels for each of the IG FISMA Reporting Metric questions as determined based on tour performance audit. We included these maturity levels in CyberScope responses made on behalf of the Interior 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 the Interior. 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 the Interior'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 2)
- Respond Function: IR – Consistently Implemented (Level 3)
- Recover Function: CP - Consistently Implemented (Level 3)

Consistent with applicable FISMA requirements, OMB policy, and NIST standards, the Interior established and maintained its information security program and practices in the five Cybersecurity Functions of Identify, Protect, Detect, Respond, and Recover. However, the Interior's overall information security program was not effective as we identified deficiencies in four of the five Functions and six of the nine Domains.

We assessed the cybersecurity Detect Function as Defined (Level 2) and the Identify, Protect, 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 [redacted] of its GFEs through DHS' CDM program.

The Interior did not [redacted].

The Interior and its Bureaus and Offices can improve their RM program 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. [redacted].

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] maintained open Plans of Action and Milestones (POA&M) for the lack of a software asset management capability to track and manage software assets and licenses.

The Interior and its Bureaus and Offices can improve their RM program 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 Interior-wide software asset management (or Mobile Device Management) capability and are subject to the monitoring processes defined within the Interior's ISCM strategy. [redacted].

4. To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions including for high value assets?

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

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?

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.

The Interior and its Bureaus and Offices did not implement a consistent process to monitor the effectiveness of risk responses to the cybersecurity landscape to ensure that risk tolerances are maintained.

The Interior and its Bureaus and Offices can improve their RM program by utilizing the results of its system level risk assessments, along with other inputs, to perform and maintain an Interior-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 Interior's enterprise risk management program. The Interior should consistently monitor the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The Interior 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.

6. To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk including risk from the organization's supply chain?

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

The Interior and its Bureaus and Offices have not fully integrated their security architecture with their systems development lifecycle to include the Information and Communications Technology (ICT) supply chain.

The Interior and its Bureaus and Offices can improve their RM program by ensuring their information security architecture is integrated with their systems development lifecycle and defines and directs implementation of security methods, mechanisms, and capabilities to both the Information and Communications Technology (ICT) supply chain and the bureau and office information systems.

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: Managed and Measurable (Level 4). The organization ensures that cybersecurity risk management information is integrated into ERM reporting tools (such as a governance, risk management, and compliance tool), as appropriate.

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.

[redacted], [redacted], and [redacted] have not developed SCRM plans and procedures. The Interior and its Bureaus and Offices have not fully implemented SCRM-related policies and procedures to include the assessment and review of the supply chain related risks and evaluation of security and supply chain controls of systems or services provided by contractors or other entities on behalf of the Interior.

The Interior and its Bureaus and Offices can improve their SCRM program 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, the Interior should 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 Interior meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, the Interior should maintain visibility into its upstream suppliers and consistently track changes in suppliers.

15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?

Maturity Level: Defined (Level 2) The organization has defined and communicated its component

authenticity policies and procedures. At a minimum the following areas are addressed:

- Procedures to detect and prevent counterfeit components from entering the system.
- Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.
- Requirements and procedures for reporting counterfeit system components.

The Interior and its Bureaus and Offices have not developed and implemented anti-counterfeit policies and procedures and has not provided component authenticity and anti-counterfeit training for designated personnel.

The Interior and its Bureaus and Offices can improve their SCRM program by ensuring that they consistently implement their component authenticity policies and procedures. Further, the Interior should:

- Provide component authenticity/anti-counterfeit training for designated personnel.
- Maintain configuration control over Interior-defined system component that are awaiting repair and service or repaired components awaiting return to service.

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated and implemented across the agency and appropriately resourced?

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

[redacted] and [redacted] maintained open POA&Ms for the lack of a configuration management plan or defined and documented configuration management roles and responsibilities.

The Interior and its Bureaus and Offices can improve their CM program by ensuring resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders should be held accountable for carrying out their roles and responsibilities effectively.

18. To what extent does the organization use an enterprise wide configuration management plan that includes at a minimum the following components: roles and responsibilities including establishment of a Change Control Board (CCB) or related body; configuration management processes including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?

Maturity Level: Consistently Implemented (Level 3). The organization has consistently implemented an organization-wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization uses lessons learned in implementation to make improvements to its plan.

[redacted] and [redacted] maintained open POA&Ms for the lack of a configuration management plan to include configuration management roles and responsibilities and activities.

The Interior and its Bureaus and Offices can improve their CM program by ensuring that they monitor, analyze, and report to stakeholders' qualitative and quantitative performance measures on the effectiveness of their configuration management plans, use this information to take corrective actions when necessary, and ensure that data supporting the metrics is obtained accurately,

consistently, and in a reproducible format.

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], [redacted], and [redacted] maintained open POA&Ms for the lack of a documented processes over security related configuration changes and baselines. This metric was not applicable for [redacted], [redacted] and [redacted] as a third-party vendor was responsible for flaw remediation and patch management for the in-scope information system.

The Interior and its Bureaus and Offices can improve their CM program by consistently implementing, assessing, and maintaining secure configuration settings for their information systems based on the principle of least functionality. Further, the Interior should consistently use Security Content Automation Protocol (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. The Interior should 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] did not consistently remediate vulnerabilities in accordance with the Interior Risk Management Policies. [redacted] and [redacted] maintained open POA&Ms to address weaknesses relating to patch management and vulnerability management, respectively. This metric was not applicable for [redacted], [redacted], and [redacted] as a third-party vendor was responsible for flaw remediation and patch management for the in-scope information systems.

The Interior and its Bureaus and Offices can improve their CM program by implementing flaw remediation policies, procedures, and processes and ensuring patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the Interior should patch critical vulnerabilities within [redacted] 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, the Interior should use supported software versions.

23. To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB as appropriate?

Maturity Level: Defined (Level 2). The organization has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.

[redacted] did not consistently manage configuration changes in accordance with the Interior and [redacted] policies and procedures. [redacted] maintained open POA&Ms for the lack of configuration management procedures. This metric was not applicable to [redacted] and [redacted] as a third-party vendor was responsible for configuration changes for the in-scope system.

The Interior and its Bureaus and Offices can improve their CM program by implementing their change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation. The Interior should use lessons learned in implementation to make improvements to its change control policies and procedures.

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?

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

The Interior and its Bureaus and Offices did not employ automation to centrally document, track, and share risk designations and screening information with necessary parties.

The Interior and its Bureaus and Offices can improve their IAM program by employing automation to centrally document, track, and share risk designations and screening information with necessary parties.

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.

[redacted] maintained an open POA&M for the lack of multifactor authentication mechanisms for the

in-scope 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 provision privileged access to the in-scope systems in accordance with account management procedures. [redacted] did not consistently review privileged accounts in accordance with Interior and [redacted] policies and procedures. [redacted], [redacted], [redacted], and [redacted] did not consistently implement audit log and review policies and procedures.

The Interior and its Bureaus and Offices can improve their IAM program by ensuring that their processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the Interior. The Interior should limit the functions that can be performed when using privileged accounts, limit the duration during which privileged accounts can be logged in, and ensure that privileged user activities are logged and periodically reviewed.

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] maintained an open POA&M for the lack of an encryption mechanism for data in transit.

The Interior and its Bureaus and Offices can improve their DPP program by ensuring the security controls for protecting PII and other Interior sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the Interior's ISCM strategy.

37. To what extent has the organization implemented security controls (e.g., Endpoint Detection 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.

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

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

38. To what extent has the organization developed and implemented a Data Breach Response Plan as appropriate to respond to privacy events?

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

The Interior did not document and define qualitative or quantitative performance metrics to measure the effectiveness of its Data Breach Response Plan.

The Interior can improve its DPP program by monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. The Interior should ensure that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals including role-based privacy training?

Note: Privacy awareness training topics should include as appropriate: responsibilities under the Privacy Act of 1974 and E Government Act of 2002 consequences for failing to carry out responsibilities identifying privacy risks mitigating privacy risks and reporting privacy incidents data collections and use requirements)

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

The Interior did not measure the effectiveness of its privacy awareness training program by obtaining feedback on privacy training.

The Interior can improve its DPP program by measuring the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the Interior should make updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.

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.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission risk environment and types of information systems? (Note: awareness training topics should include as appropriate: consideration of organizational policies roles and responsibilities secure e-mail browsing and remote access practices mobile device security secure use of social media phishing malware physical security and security incident reporting?

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

The Interior did not define qualitative and quantitative performance measures to assess the effectiveness of its security awareness policies and procedures.

The Interior can improve its ST program by measuring the effectiveness of its awareness program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. The Interior should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices. The Interior should obtain that data supporting metrics accurately, consistently, and in a reproducible format.

45. To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?

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

The Interior did not obtain feedback or measure the effectiveness of its specialized security training content and processes. [redacted] did not remove network access from individuals that did not complete the annual specialized security training.

The Interior can improve its ST program by obtaining feedback on its specialized security training content and processes and make updates to its program, as appropriate. In addition, the Interior should measure the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional training, and/or disciplinary action, as appropriate. The Interior should monitor and analyze qualitative and quantitative performance measures on the effectiveness of its security training policies, procedures, and practices. The Interior should obtain data supporting metrics 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] maintained an open POA&M to address the implementation of its ISCM plan. The Interior did not define qualitative or quantitative performance metrics to measure the effectiveness of its ISCM policies and strategy.

The Interior and its Bureaus and Offices can improve their ISCM program by monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and makes updates, as appropriate. The Interior should obtain data supporting metrics accurately, consistently, and in a reproducible format. The Interior should transition to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.

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: Consistently Implemented (Level 3). The organization consistently implements its system-level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining

system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. In conjunction with the overall ISCM strategy, all security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status updated regularly (as defined in the agency's information security policy) in security plans.

[redacted] maintained an open POA&M to address the implementation of its ISCM plan.

The Interior and its Bureaus and Offices can improve ISCM program by utilizing the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. The Interior's authorization processes should include automated analysis tools and manual expert analysis, as appropriate.

50. How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?

Maturity Level: Defined (Level 2) The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, the organization has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.

The Interior and its Bureaus and Offices did not define qualitative or quantitative performance metrics to measure the effectiveness of the ISCM strategy. [redacted] maintained an open POA&M to address the implementation of its ISCM plan.

The Interior and its Bureaus and Offices can improve their ISCM program by consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.

52. To what extent does the organization use an incident response plan to provide a formal focused and coordinated approach to responding to incidents?

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

The Interior and its Bureaus and Offices did not monitor and analyze quantitative or qualitative performance measures to assess the effectiveness of the incident response capability.

The Interior and its Bureaus and Offices can improve their IR program by monitoring and analyzing the qualitative and quantitative performance measures that have been defined in the incident response plan to monitor and maintain the effectiveness of the overall incident response capability. The Interior should obtain data supporting metrics accurately, consistently, and in a reproducible format.

53. To what extent have incident response team structures/models stakeholders and their roles responsibilities levels of authority and dependencies been defined 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 incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.

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

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.

The Interior and its Bureaus and Offices did not meet the logging requirements of the maturity Event Logging [redacted], in accordance with OMB Memorandum M-21-31.

The Interior and its Bureaus and Offices can improve IR program by implementing the [redacted] 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.

The Interior did not monitor and analyze quantitative or qualitative performance measures to assess the effectiveness of the incident handling policies and procedures.

The Interior and its Bureaus and Offices can improve their IR program by monitoring and analyzing qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The Interior should obtain data supporting metrics accurately, consistently, and in a reproducible format. The Interior should manage and measure the impact of successful incidents and quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.

56. To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?

Maturity Level: Consistently Implemented (Level 3). The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to US-CERT, law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident reporting policies and procedures and making updates as necessary.

The Interior and its Bureaus and Offices did not define metrics to measure the timely reporting of incident information to organizational officials and external stakeholders.

The Interior and its Bureaus and Offices can improve their IR program by ensuring incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. The Interior should obtain data supporting metrics accurately, consistently, and in a reproducible format.

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

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

[redacted] maintained an open POA&M for the lack of policies and procedures related to the contingency planning program, to include the management of Business Impact Analysis. This metric was not applicable for [redacted] as it was addressed through processes and controls implemented and managed by a third-party vendor.

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

62. To what extent does the organization ensure that information system contingency plans are developed maintained and integrated with other continuity plans?

Maturity Level: Consistently Implemented (Level 3). The organizations Information system contingency plans are consistently developed and implemented for systems, as appropriate, and include organizational and system-level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system-level contingency planning development/maintenance activities are integrated with other continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.

[redacted] maintained an open POA&M for the lack of policies and procedures related to the contingency program. This metric was not applicable for [redacted] as it was addressed through processes and controls implemented and managed by a third-party vendor.

The Interior and its Bureaus and Offices can improve their CP program by integrating metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as those that support organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as

appropriate, to deliver persistent situational awareness across the organization. The Interior should coordinate the development of ISCPs with the contingency plans of external service providers.

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] maintained an open POA&M for the lack of a contingency planning program. This metric was not applicable for [redacted] as it was addressed through processes and controls implemented and managed by a third-party vendor.

The Interior and its Bureaus and Offices can improve their CP program by employing automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the Interior should coordinate plan testing with external stakeholders (e.g., ICT supply chain partners/providers), as appropriate.

64. To what extent does the organization perform information system backup and storage including use of alternate storage and processing sites as appropriate?

Maturity Level: Consistently Implemented (Level 3). The organization consistently implements its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments that ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized. In addition, the organization ensures that these sites and are not subject to the same risks as the primary site. Furthermore, the organization ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site, including applicable ICT supply chain controls. Furthermore, backups of information at the user- and system-levels are consistently performed, and the confidentiality, integrity, and availability of this information is maintained.

[redacted] maintained an open POA&M for the lack of a contingency planning program. This metric was not applicable for [redacted] as it was addressed through processes and controls implemented and managed by a third-party vendor.

The Interior and its Bureaus and Offices can improve their CP program by ensuring that its information system backup and storage processes, including use of alternate storage and processing sties, and related supply chain controls, are assessed, as appropriate, as part of its continuous monitoring program.

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.

WHO CAN REPORT?

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement involving 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 OIG, and the information they share can lead to reviews and investigations that result in accountability and positive change for 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. Specifically, 5 U.S.C. § 407(b) 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.

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