EVALUATION

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

The U.S. Department of the Interior's Cyber Risk Management Practices Leave Its Systems at Increased Risk of Compromise

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

Report No.: 2020–ITA–030 February 2023

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

FEB 2 8 2023

Memorandum

To: Darren Ash
Chief Information Officer

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

Subject: Final Evaluation Report – *The U.S. Department of the Interior's Cyber Risk Management Practices Leave Its Systems at Increased Risk of Compromise*
Report No. 2020–ITA–030

This memorandum transmits our evaluation report on the U.S. Department of the Interior's (DOI's) information system risk management practices for authorizing systems to operate.

We will refer Recommendations 1 through 11 to the Office of Policy, Management and Budget for implementation tracking and to report to us on their status. In addition, we will notify Congress about our findings, and we will report semiannually, as required by law, on actions you have taken to implement the recommendations and on recommendations that have not been implemented. We will also post a public version of this report on our website.

If you have any questions about this report, please call me at 202–208–5745.

cc: John Clink, Acting Chief Information Security Officer

Contents

Report Abbreviations 1

Results in Brief 2

Introduction 4

- Objective 4
- Background 4
  - Federal Standards 4
  - DOI Policies and Practices 6

Results of Evaluation 8

- The DOI Did Not Ensure Its Operational Systems Were Authorized or Included in Its Annual Audits or Assurance Statements 8
  - DOI Information Systems Were Operating Without Authorization 9
  - Some DOI Operational Information Systems Were Incorrectly Omitted From FISMA Audit or Annual Assurance Statements 11
- The DOI Did Not Implement Appropriate Security Control Testing and Review 12
- The DOI Did Not Ensure Timely and Complete Remediation of Security Weaknesses 14
- The DOI Did Not Properly Assess and Document All Systems Containing Personally Identifiable Information 16

Conclusion and Recommendations 18

- Conclusion 18
- Recommendations Summary 18

Appendix 1: Scope and Methodology 23

- Scope 23
- Methodology 23

Appendix 2: Response to Draft Report 25

Appendix 3: Status of Recommendations 31

Report Abbreviations

Annual Assurance Statement (AAS)

Authorization to Operate (ATO)

Bureau of Land Management (BLM)

Bureau of Trust Funds Administration (BTFA)

Cyber Security Assessment and Management (CSAM)

U.S. Department of the Interior (DOI)

Federal Information Security Modernization Act of 2014 (FISMA)

National Institute of Standards and Technology (NIST)

National Park Service (NPS)

Office of the Chief Information Officer (OCIO)

Office of Management and Budget (OMB)

U.S. Office of Personnel Management (OPM)

Office of the Secretary (OS)

Office of Surface Mining Reclamation and Enforcement (OSMRE)

Privacy Impact Assessment (PIA)

Personally Identifiable Information (PII)

Plans of Action and Milestones (POA&Ms)

Special Publication (SP)

Results in Brief

What We Reviewed

Protecting Federal computer networks and data from cyber threats remains one of the most serious economic and national security challenges facing our Nation. The U.S. Department of the Interior (DOI) stores and maintains critical data related to mission-related topics such as hydroelectric dams, oil and gas infrastructure, security at national parks, geospatial satellites, and law enforcement activities. Conducting accurate risk assessments and addressing security risks in a timely manner are essential components of ensuring the safety of the DOI's critical data.

We evaluated the DOI's information system risk management practices to determine if the DOI has appropriately authorized its systems to operate and if the DOI analyzed and monitored security weaknesses to reduce the risk of compromise. Specifically, we evaluated whether the DOI authorized systems for operation based on complete and accurate risk assessments. We also evaluated risk assessment remediation plans (Plans of Action and Milestones or POA&Ms) to determine whether the DOI, through its bureaus and offices, addressed and mitigated security weaknesses in a timely manner, closed the POA&Ms appropriately, and continuously monitored and tracked the plans.

What We Found

We found that DOI systems were operating without authorization and that the DOI did not consistently analyze and monitor security weaknesses. Due to the DOI's lack of resource prioritization and clear guidelines, the Federal information systems under its responsibility are at an increased risk of compromise. Specifically, we reviewed 38 systems and found the following:

- Nine systems (24 percent) were operating without authorization or were missing annual audits or assurance statements.

- Seven systems (18 percent) were incorrectly excluded from the required annual Federal Information Security Modernization Act audit.

- Seventeen systems (45 percent) did not implement required security controls or conduct ongoing security control testing.

- Nineteen systems (50 percent) did not remediate vulnerable security weaknesses identified in their POA&Ms, which were marked as "delayed" and were not remediated and closed out by their scheduled due dates.

- Twenty-three systems (61 percent) with personally identifiable information did not have properly documented and assessed privacy controls.

These deficiencies occurred because the Office of the Chief Information Officer lacks a comprehensive quality control program, which would ensure that system security documentation is complete, accurate, and up to date.

Why This Matters

DOI systems are at increased risk of compromise because of systems that are operating without authorization or without appropriate oversight of security controls and weakness. In recognition of these risks, managing and securing IT networks and operations continues to be one of the top management and performance challenges facing Federal agencies, including the DOI. The DOI cannot make informed enterprise risk management decisions without accurate information regarding the security status of its systems

What We Recommend

We make 11 recommendations to help strengthen the DOI's information system risk management practices and information system security.

Introduction

Objective

We evaluated the U.S. Department of the Interior's (DOI's) information system risk management practices to determine if the DOI has appropriately authorized its systems to operate and if the DOI analyzed and monitored security weaknesses to reduce the risk of compromise. Specifically, we evaluated whether the DOI authorized systems for operation based on complete and accurate risk assessments. We also evaluated Plans of Action and Milestones (POA&Ms) to determine whether the DOI, through its bureaus and offices, addressed and mitigated security weaknesses in a timely manner, closed the POA&Ms appropriately, and continuously monitored and tracked the plans.

Appendix 1 provides further details on our scope and methodology.

Background

In June 2015, the U.S. Office of Personnel Management (OPM) announced[1] that it had been the target of a data breach. Specifically, nation-state actors[2] accessed and exfiltrated approximately 22.1 million records related to Federal background checks, including personally identifiable information. The OPM Office of the Inspector General's *Semiannual Report to Congress*, issued in June 2015, warned of "persistent deficiencies in OPM's information system security program," including "incomplete security authorization packages, weaknesses in testing of information security controls, and inaccurate Plans of Action and Milestones."[3] This breach is one significant example that exemplifies the possible consequences of a poor information system security program. Many Federal standards and DOI policies address these risks.

Federal Standards

The Federal Information Security Modernization Act of 2014 (FISMA)[4] establishes guidelines and security standards to protect Government information and operations—an essential part of reducing the risk of attacks such as the OPM breach. FISMA defines specific information security requirements Federal agencies must satisfy and assigns responsibilities to senior agency officials and agency inspectors general for satisfying FISMA requirements. Specifically, FISMA requires the Secretary or equivalent of each Department to administer the implementation of agency information security policies and practices for information systems in coordination and

[1] OPM, *OPM to Notify Employees of Cybersecurity Incident*, available at https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.

[2] A nation-state actor is a hacker or group of hackers working with an adversarial government that commits acts of cybercrime against the United States or its allies (https://www.techtarget.com/searchsecurity/news/252499613/The-wide-web-of-nation-state-hackers-attacking-the-US).

[3] OPM Office of the Inspector General *Semiannual Report to Congress October 1, 2014–March 31, 2015*, available at https://oig.opm.gov/reports/semiannual/semiannual-report-congress-october-1-2014-march-31-2015.

[4] Federal Information Security Modernization Act, Pub. L. No. 113–283, available at https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

consultation with the Director of the National Institute of Standards and Technology (NIST). FISMA also requires agencies to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency information assets.

According to NIST guidance, Federal computer systems are categorized as either low-, moderate-, or high-impact security systems, a designation that again is commensurate with the risk and magnitude of harm should the system be compromised.[5] For example, a low-impact system security breach could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A moderate-impact system breach could be expected to have a serious or severe adverse effect. For high-impact systems, the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect. The system security categorization also prescribes the minimum controls that must be implemented to help ensure the availability of the computer system, as well as the confidentiality and integrity of the sensitive data it contains.

Office of Management and Budget (OMB) policy[6] explains that the Authorization to Operate (ATO) is the formal risk evaluation and acceptance process that drives the decision to allow a system to store and process data. Specifically, the system owner[7] must test the system's security controls to ensure the controls are implemented correctly, operating as intended, and producing the desired outcome of protecting the system and its data from loss or disruption before the authorizing official[8] can authorize a system to operate. Moreover, responsible officials must consider the number, significance, and implementation status of open corrective action plans, or POA&Ms, before authorizing a system for operation. The authorizing official, in conjunction with the system owner, relies on the system security categorization level, security control test results, and the open POA&M status to make a risk-based decision on whether to authorize a system for operation. By authorizing a system for operation, the authorizing official and system owner accept responsibility for the security of the system and are fully accountable for any adverse effects to the DOI if a system breach occurs.

As part of meeting the requirements of FISMA as well as the Federal Managers Financial Integrity Act of 1982,[9] bureau and office heads must review and approve annual assurance

---

[5] NIST Federal Information Processing Standards Publication 199: *Standards for Security Categorization of Federal Information and Information Systems*, available at https://csrc nist.gov/publications/detail/fips/199/final; and NIST Special Publication (SP) 800–60 Volume 1, Revision 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*, available at https://csrc nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final.

[6] OMB Circular No. A–130, *Managing Information as a Strategic Resource*, revised July 2016, available at https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/OMB-A-130.

[7] A system owner is– a person or organization responsible for the development, procurement, integration, modification, operation, maintenance, or final disposition of an information system. *See* NIST SP 800–161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, available at https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf.

[8] An authorizing official is an official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority. *See* NIST SP 800-60 Volume 1, Revision 1.

[9] Federal Managers Financial Integrity Act of 1982, Pub. L. No. 97–255, available at https://uscode house.gov/statutes/pl/97/255.pdf.

statements attesting to the effectiveness of implemented security controls, status of corrective actions for open POA&Ms, and accuracy of information in the official repository of information systems and related security documentation for all IT systems under their purview. Specifically, bureau and office heads must attest annually that, for all operational IT systems, the system owners have:

- Completed a test of the system's security controls.
- Taken corrective actions to address open POA&Ms.
- Documented accurate information in the repository (including IT system operational status, FISMA reportability, system type, and ATO status).

DOI Policies and Practices

The DOI's Office of the Chief Information Officer (OCIO) is responsible for developing and overseeing DOI-wide, risk-based, and cost-effective policies and procedures for addressing information security. Senior officials within the DOI's bureaus and offices are responsible for enforcing security policies and procedures by assessing potential risks and implementing operational and technical controls that mitigate identified risks to DOI information systems.

One example of a risk mitigation method is the annual assurance statement process, which the bureaus and offices use to assure that internal control self-assessment results and documentation are accurately recorded in the DOI's official repository of information systems to help the DOI make risk-based decisions. Senior officials at the bureaus and offices are also responsible for implementing controls and testing and evaluating information security controls to ensure continued compliance with DOI standards. Each bureau and office, including the OCIO, has both system owners and authorizing officials for their respective information systems. The DOI's Office of Inspector General or an independent external auditor performs an annual audit of the DOI's information security practices in accordance with the U.S. Department of Homeland Security's and the OMB's FISMA reporting instructions.

Security controls are the management, operational, and technical safeguards that help ensure the confidentiality, integrity, and availability of an IT system and its data. If the DOI's security controls do not function as intended, the DOI could experience a system breach resulting in the loss of sensitive information or an adverse effect on Department operations. Pursuant to NIST and DOI policy, when IT security deficiencies are identified, system owners must create POA&Ms documenting the planned remediation process if the deficiencies cannot be mitigated.[10] POA&Ms assist DOI officials in identifying, assessing, prioritizing, and monitoring the progress of efforts to correct IT security weaknesses found in DOI systems and programs.

[10] NIST SP 800–37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, available at https://csrc nist.gov/publications/detail/sp/800-37/rev-2/final; NIST SP 800–53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, issued April 2013, available at https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; and DOI *Plan of Action and Milestones Process Standard*.

These plans are also used to close security performance gaps and assist OIG staff when evaluating the DOI's security performance.

The Cyber Security Assessment and Management (CSAM) system is the DOI's official repository of information systems and related security documentation. CSAM provides the OCIO and relevant bureau and office personnel with a DOI-wide view of the status of information system security and documented processes, including tests of security controls, status of POA&Ms, and privacy risks. This centralized view assists the CIO and staff in performing enterprisewide risk evaluations and making agencywide IT decisions based on the residual risk of all systems within the DOI. Without this view, management could potentially approve or implement changes that introduce or exacerbate cyber threats.

To determine whether authorizing officials have appropriately authorized the DOI's systems to operate and documented and closed security weaknesses with effective mitigations in place, we selected a sample of 38 of the DOI's 222 systems (17 percent) from CSAM for review with a security categorization distribution of 6 low, 31 moderate, and 1 high.[11]

[11] See Appendix 1 for additional information on our sample selection.

Results of Evaluation

We found that multiple DOI systems were operating without authorization and that the DOI did not consistently analyze and monitor security weaknesses. These deficiencies, which we attribute to a lack of resource prioritization and clear guidelines, mean that the Federal information systems under the DOI's responsibility are at an increased risk of compromise.

Specifically, we reviewed 38 systems and found the following:

- Nine systems (24 percent)—six categorized as moderate impact and three as low impact—were operating without authorization or were missing annual audits or assurance statements.

- Seven systems (18 percent)—five categorized as moderate impact and two as low impact—were incorrectly excluded from the required annual FISMA audit.

- Seventeen systems (45 percent)—1 categorized as high impact, 13 as moderate impact, and 3 as low impact—did not implement required security controls or conduct ongoing security control testing.

- Nineteen systems (50 percent) with security weaknesses—1 categorized as high impact, 17 as moderate impact, and 1 as low impact—had POA&Ms marked as "delayed" that were not remediated and closed out by their scheduled due dates.

- Twenty-three systems (61 percent) with personally identifiable information did not have properly documented and assessed privacy controls.

These deficiencies occurred because the OCIO lacks a comprehensive quality control program that would ensure that system security documentation is complete, accurate, and up to date. The DOI cannot make informed enterprise risk management decisions without accurate information regarding the security status of systems within the DOI. In addition, the Federal information systems under its responsibility are at an increased risk of compromise. Our findings cast doubt on the validity of the entire assurance process and demonstrate the need for sustained oversight at the bureau, office, and DOI levels.

The DOI Did Not Ensure Its Operational Systems Were Authorized or Included in Its Annual Audits or Assurance Statements

We found that nine systems were either operating without ATOs or were missing annual audits or assurance statements (see Figure 1). Specifically, seven systems were operating without ATOs. In addition, five of the nine systems were incorrectly excluded from annual FISMA audit because they were not designated as "operational" in CSAM. We also found that two additional systems were excluded from both FISMA audit and the DOI's annual assurance statements. This occurred because the DOI did not ensure that system security documentation was complete,

accurate, and up to date. A review of each system's operational status, authorization paperwork, and the completeness of system documentation would have identified systems operating without an ATO and systems that had been incorrectly excluded from annual FISMA audit or annual assurance statements.

Figure 1: Status of Systems Operating Without Authorization, FISMA Audit, or Annual Assurance Statements

System	Bureau/ Office	ATO (Y/N)	FISMA Audit (Y/N)	AAS (Y/N)
System 1	BLM	N	Y	Y
System 2	BTFA	N	N	N
System 3	NPS	N	N	N
System 4	OS	Y	N	Y
System 5	OS	Y	N	N
System 6	OS	N	N	N
System 7	OS	N	N	N
System 8	OS	N	N	N
System 9	OSMRE	N	Y	N

DOI Information Systems Were Operating Without Authorization

OMB policy[12] mandates that all Federal information systems have a valid ATO, which is the official management decision given by a senior Federal official to authorize operation of an information system and to explicitly accept the risk to agency operations, assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security and privacy controls. This is intended to prevent the introduction of unacceptable risk to the organization. We found that 7 of the 38 systems we reviewed (16 percent), including 4 moderate-impact systems, were operating without the required ATO (see Figure 2). According to NIST, a breach of a moderate-impact system could be expected to have a serious adverse effect on organizational operations, assets, or individuals.

[12] OMB Circular A–130, Appendix I § 4(d), revised July 2016.

Figure 2: DOI Systems Operating Without an ATO

System	Bureau / Office	Impact
System 1	BLM	Moderate
System 2	BTFA	Low
System 3	NPS	Low
System 6	OS	Moderate
System 7	OS	Moderate
System 8	OS	Low
System 9	OSMRE	Moderate

NIST and OMB guidance require the DOI to implement a risk management framework.[13] Moreover, the NIST guidelines provide a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

Even though the DOI incorporates NIST's process into its *Security Assessment Standard* to evaluate whether system security controls meet security requirements before they are deployed, DOI systems nonetheless operated without ATOs. This means that the DOI did not appropriately assess and accept any risks associated with operating the system. This occurred, in part, because the DOI's annual assurance process failed to identify systems operating without required ATOs due to a lack of DOI-level quality control measures. Federal laws and OMB policy[14] require the CIO to assess information security controls. DOI policy[15] also requires the CIO to issue a consolidated assurance statement regarding internal controls over information and technology. The CIO, however, relied solely on the bureau and office assurance statements to develop the DOI's consolidated assurance statement and determine the DOI's residual risk. The CIO did not have processes in place to confirm the information provided by the bureaus and offices.

When we informed the OCIO of these issues, the OCIO, bureaus, and offices addressed them by completing ATOs for systems, moving systems under appropriate operational parents, or retiring systems entirely.

[13] NIST SP 800–37, Revision 2, Chapter 3, "The Process: Executing the Risk Management Framework Tasks," available at https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[14] Federal Managers' Financial Integrity Act of 1982; OMB Circular A–123, *Management's Responsibility for Internal Control*, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf; and FISMA.

[15] DOI Financial Management Memorandum 2020–005, *Guidance for the Fiscal Year 2020 Internal Control Program.*

Recommendation

We recommend that the OCIO:

1. Develop and implement a process to evaluate all systems' Authorizations to Operate annually for accuracy and completeness to ensure systems are operating with a valid authorization determined by actual residual risk.

Some DOI Operational Information Systems Were Incorrectly Omitted From FISMA Audit or Annual Assurance Statements

FISMA requires that all operational agency information systems be included in the population of information systems from which a representative sample is selected. This sample of information systems undergoes the annual FISMA audit.

The DOI's annual FISMA audit includes systems that are sampled based on operational and ATO status. DOI staff designate the operational status of a system within CSAM. This designation determines whether a system may be included when the third-party independent auditor selects its sample for FISMA compliance. We found 7 of the 38 operational systems we reviewed (18 percent) were incorrectly excluded from annual FISMA audit (see Figure 3). In addition, of these seven operational systems, we found that six were not listed in their bureau or office annual assurance statements.

Figure 3: Systems Incorrectly Excluded from Annual FISMA Audit

System	Bureau/Office	Impact	ATO (Y/N)
System 2	BTFA	Low	N
System 3	NPS	Low	N
System 4	OS	Moderate	Y
System 5	OS	Moderate	Y
System 6	OS	Moderate	N
System 7	OS	Moderate	N
System 8	OS	Low	N

The seven systems that were excluded from FISMA audits were designated in CSAM as "under development"; however, interviews with the respective system owners confirmed that the systems were operational. Four of the seven systems were categorized as moderate impact, meaning that a system breach could be expected to have a serious adverse effect on bureau operations, assets, or individuals. The remaining three systems were categorized as low impact.[16] Finally, five of the seven systems were operating without an ATO.

[16] Low-impact systems are easily replaced, and the information stored is not private or sensitive.

Because the DOI did not properly designate seven systems as operational in CSAM, those systems were not included in the population sample for an independent audit of whether the security controls in the systems were implemented correctly, operating as intended, and producing the desired outcome of protecting the system and data from loss or disruption. As noted earlier, the DOI did not conduct its own quality control reviews. If it had conducted the appropriate reviews, it could have identified the incorrect designations in CSAM and included those systems in the annual FISMA audit.

In addition, the DOI's annual assurance statement process described previously applies to all information systems currently in use by DOI bureaus or offices and assures that internal control self-assessment results and documentation are accurately recorded in CSAM. The Department, however, relied on the bureau and office assurance statements without conducting quality control reviews or other validation to ensure the statements were accurate. For the six operational systems that were excluded from the annual assurance statement, the DOI has no assurance that the systems' security controls are effective for protecting the systems from loss or disruption or the status of corrective actions to address any open POA&Ms. As four of the six systems are moderate impact, a system breach could be expected to have a serious adverse effect on bureau or office operations, assets, or individuals.

Recommendations

We recommend that the OCIO:

2. Develop and implement a process to conduct quality control reviews at least annually to ensure that all systems within the official system of record (Cyber Security Assessment and Management system) have an accurate operating status.

3. Develop and implement a process to validate the accuracy of bureau and office annual assurance statements before submitting the statements to Congress.

The DOI Did Not Implement Appropriate Security Control Testing and Review

We found that the DOI did not implement required security controls or conduct ongoing security control testing, resulting in assessment deficiencies in 17 of the 38 systems we reviewed (45 percent).

NIST guidance[17] provides all agencies with more than 1,000 security controls for a comprehensive, flexible, repeatable, and measurable process that they can use to manage information security and privacy risk for its IT systems. Each system has a set of baseline controls and recommended additional controls that the system owner and authorizing official

[17] NIST SP 800–53.

select when developing a new system. A control is documented as implemented when the system has been used and an independent reviewer has assessed the security control.

We found that system owners documented only 54 percent of the required controls as not implemented and had not tested 22 percent of controls in more than 3 years, which was the requirement before a March 2012 switch to continuous monitoring of the controls.[18] The DOI allowed these systems to operate even though the system owners did not complete required system security control documentation and testing for effectiveness at protecting the system and its data.

Additionally, the system owners did not update documentation of the results of security tests in CSAM as required by DOI policy.[19] These results funnel into the bureau and office annual assurance statement process; however, if the system owners do not update the documentation, the DOI cannot accurately assess system security risks. This deficiency occurred because the DOI did not ensure that bureaus and offices performed quality control for the data entered into their official systems of record.

Again, the DOI's annual assurance process did not identify flawed systems due to a lack of DOI-level quality control and bureau or office quality control measures. Had the bureaus and offices conducted a quality review before submitting the assurance statements and had the DOI conducted a review after the bureaus submitted the assurance statements, the DOI may have been able to identify these system issues.

Without complete and accurate tests of security controls, authorizing officials cannot make informed decisions on whether system owners sufficiently mitigated risks, and thus, cannot justify authorizing the systems for continued operation.

[18] DOI policy now requires bureaus and offices to conduct ongoing authorization based on continuous monitoring that assesses security controls and analyzes organization risks with a frequency sufficient to support risk-based security decisions to adequately protect organizational information.

[19] OCIO Directive 2011–006, *Information System Boundary Assessment & Authorization Package Documentation and Inventory*.

Recommendations

We recommend that the OCIO:

4. In addition to ongoing continuous monitoring, develop and implement a policy to direct system owners to test all of the controls for their systems at least every 3 years.

5. Develop and implement a policy to ensure data and control implementation status are accurately represented in the official system of record.

6. Develop and implement a policy to verify that bureaus and offices perform control assessments every 3 years.

7. Develop and implement a review process that includes, at minimum, verifying that system owners have completed required testing for a sample of controls for each system before accepting the annual assurance statement.

The DOI Did Not Ensure Timely and Complete Remediation of Security Weaknesses

The POA&M process is a management tool for identifying, tracking, and prioritizing remedial actions to ensure vulnerabilities are addressed in a timely and cost-effective manner. We found the DOI did not perform oversight of POA&M activities to ensure timely and complete remediation of security weaknesses. Specifically, for the 38 systems we reviewed, we selected 73 associated POA&Ms and reviewed their status in CSAM—as noted previously, this is the DOI's official system of record for documenting and managing system and enterprise risk.

An effective POA&M process helps the DOI ensure that security control weaknesses do not result in the unauthorized access, use, disruption, disclosure, modification, or destruction of mission-critical systems and data. According to DOI policy,[20] NIST guidance,[21] OMB policy,[22] and recognized best practices, POA&Ms must be reported to the authorizing official once per quarter. However, we found that the DOI's processes for managing POA&Ms failed to timely address security weaknesses, monitor progress, and completely document remediation efforts.

DOI policy[23] requires that, once per quarter, bureaus and offices review their POA&Ms, update their milestones, and document remediation evidence and their POA&M review results. Although we found that 88 percent of the POA&Ms reviewed (64 of 73) had milestones that appropriately documented the steps needed to remediate the security weaknesses, the DOI did

[20] OCIO Directive 2011–006.

[21] NIST SP 800–53.

[22] OMB Memorandum M–02–01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones,* issued October 17, 2001, available at https://www.whitehouse.gov/wp-content/uploads/2017/11/2002-M-02-01-Guidance-for-Preparing-and-Submitting-Security-Plans-of-Action-and-Milestones-1.pdf.

[23] OCIO Directive 2020–004.

not verify that bureaus and offices updated milestones quarterly or ensure they were addressing the weaknesses on a continuous basis. We also found that 55 percent of the POA&Ms (40 of 73) did not have milestones that were updated quarterly. Failure to update milestones once per quarter could result in security weaknesses not being remediated timely or appropriately prioritized for remediation.

Further, we found that 48 percent of all POA&Ms we selected for review (35 of 73) were marked "delayed" in CSAM and therefore have not yet been closed out by the scheduled due date. Six of these POA&Ms were delayed for at least 4 years (see Figure 4). These delayed POA&Ms covered 19 systems (50 percent of our sample information systems). In addition, 80 percent of the delayed POA&Ms (28 of 35) do not have the required documented explanations of their delays. Proper documentation allows the DOI to understand its current risk levels because delaying POA&Ms exposes DOI systems to extended risk.

Figure 4: POA&M Delays in CSAM

Delay	No. of POA&Ms
Less than 1 Year	16
1 Year	4
2 Years	4
3 Years	5
4 Years	6

The DOI *Plan of Action and Milestones Process Standard* and NIST guidance[24] require system owners to test mitigation before closing POA&Ms and document the testing in a Weakness Completion Verification Form. We found that 2 of the 28 POA&Ms designated as closed in CSAM did not have evidence of the required Weakness Completion Verification Form documenting that the system owner and authorizing official understand the weakness, approve of the mitigations, and approve of any residual risk should it exist. Without appropriate documentation, the OCIO cannot ensure the bureaus and offices appropriately remediated security weaknesses to warrant closing POA&Ms and cannot confirm if system owners tested mitigation or the authorizing officials approved the closures.

These issues occurred because the DOI and OCIO did not provide adequate oversight and instead relied on the system owners, authorizing officials, and bureaus that did not conduct adequate quality control. Failure to monitor POA&Ms and update milestones on a regular basis exposes the DOI to increased operational security risks and hampers the DOI's ability to effectively allocate resources to ensure timely remediation of cybersecurity weaknesses.

[24] NIST SP 800–37.

Recommendation

We recommend that the OCIO:

8. Develop and implement a comprehensive quality control plan to perform required quarterly reviews of Plans of Action and Milestones in the official system of record to ensure that bureaus and offices address them in a timely manner, close them as appropriate, and continuously monitor and track them.

The DOI Did Not Properly Assess and Document All Systems Containing Personally Identifiable Information

The E-Government Act of 2002 requires agencies to conduct Privacy Impact Assessments (PIAs) before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public, and generally make them available to the public.[25] Examples of technology systems that generally have privacy implications are human resources, payroll, and law enforcement systems. Even if it is not apparent that a system collects or maintains personally identifiable information (PII), [26] there could be instances where a new or changed connection with other systems, additional sources of data, or evolving intended use of the system may increase privacy risks. For example, NIST SP 800–53, Revision 4, introduced additional privacy controls intended to protect the PII of individuals that organizations collect and maintain in accordance with Federal privacy laws, regulations, and policies. When NIST releases new privacy controls, agencies are required to assess these new controls in established PIAs and ATOs.

The DOI's Privacy Office works with system owners to complete these PIAs—one of the key methods system owners use to determine which privacy controls are applicable to their systems.[27] However, we found that 61 percent of systems reviewed (23 of 38) did not document any privacy controls. The DOI is at increased risk of the potential loss of PII because privacy controls had not been properly assessed and documented on all systems with PII. Although the DOI's Privacy Office created policy for the required privacy controls and delegated implementation and control assessments to the bureaus, the DOI and the bureaus expressed uncertainty regarding the policy and who is responsible for both implementing and documenting the status of these security controls within CSAM. In particular, the bureaus and offices told us

[25] E-Government Act of 2002, Pub. L. No. 107–347, available at https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[26] PII is data that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual. Examples of PII include but are not limited to name, home mailing address, personal telephone number, social security number, date of birth, nationality, passport number, bank account number, and credit card number.

[27] According to NIST, privacy controls are "[t]he administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks." https://csrc.nist.gov/glossary/term/privacy_control.

they did not know who was in charge of assessing whether these controls apply to their systems or who is responsible for implementing them.

The DOI did not provide evidence that it had assessed privacy controls for the majority of systems we reviewed. Because the DOI did not follow up on how the bureaus implemented and documented the security controls within CSAM, the DOI was not aware of the missing privacy controls or issues regarding who was responsible for these controls. Lack of privacy control review leaves the DOI at greater risk of unauthorized PII exposure, which can compromise the privacy of individuals and erode public trust.

Recommendations

We recommend that the OCIO:

9. Direct system owners to perform annual reviews of the data contained in all operational IT systems to ensure that an accurate privacy impact assessment has been completed and, when necessary, adjust the system's security categorization.

10. Develop and implement a process to ensure that a Privacy Impact Assessment is conducted before a system is granted Authorization to Operate.

11. Develop and implement a policy clarifying the roles and responsibilities regarding control assessment and implementation.

Conclusion and Recommendations

Conclusion

DOI systems are at increased risk of compromise because of systems that are operating without an ATO or without appropriate oversight of security controls and weakness. We determined that the DOI did not ensure that all operational systems were authorized or included in its annual audits. We also found that systems had assessment deficiencies related to required security controls and ongoing security control testing. Additionally, we found that the DOI did not ensure timely remediation of security weaknesses, and systems with PII are at increased risk.

This occurred because the OCIO lacks a comprehensive quality control program, which would help ensure that system security documentation is complete, accurate, and up to date. The deficiencies can be alleviated by improving the quality control policy and assurance statement process at the bureau or office and DOI level before and after submission.

The current DOI assurance statement process and quality control process did not confirm that the internal controls over the effectiveness and efficiency of information systems operations complied with applicable laws and regulations and were suitably designed and operating effectively at the time the bureaus or offices signed the statements. A review of each system's operational status, authorization paperwork, and the completeness of system documentation would have identified these deficiencies.

The DOI cannot make informed enterprise risk management decisions without accurate information regarding the security status of its systems. These deficiencies hinder the appropriate prioritization of funding and staffing resources to mitigate weaknesses in DOI systems, which could result in a data breach. As evidenced by previous breaches—for example, the OPM's 2015 breach—the consequences can be significant for the Federal Government and for affected individuals alike.

Recommendations Summary

We provided a draft of this report to the DOI for review. The DOI concurred with all 11 recommendations. We consider all 11 recommendations resolved but not implemented. Below we summarize the DOI's response to our recommendations, as well as our comments on its response. See Appendix 2 for the full text of the DOI's response; Appendix 3 lists the status of each recommendation.

We recommend that the OCIO:

1. Develop and implement a process to evaluate all systems' Authorizations to Operate annually for accuracy and completeness to ensure systems are operating with a valid authorization determined by actual residual risk.

DOI Response: The DOI concurred with our recommendation and stated that the OCIO will develop a process to review ATO data "in the enterprise Governance, Risk, and Compliance (GRC) tool and alert bureaus and offices when systems are operating without valid authorization or approaching such state." The DOI also stated that the OCIO will develop customized reports for those instances in which the GRC tool does not automate generating reports. The DOI provided a target implementation date of December 15, 2023, and further noted that it anticipates the GRC tool, which is the current system of record, to change in fiscal year 2023.

OIG Comment: Based on the DOI's response, we consider Recommendation 1 resolved but not implemented.

2. Develop and implement a process to conduct quality control reviews at least annually to ensure that all systems within the official system of record (Cyber Security Assessment and Management system) have an accurate operating status.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will develop a process to review ATO data in the enterprise GRC tool and alert bureaus and offices when systems have recorded a non-operational status for an extended period." The DOI also stated that the OCIO will develop customized reports for those instances in which the GRC tool does not automate generating reports. The DOI provided a target implementation date of December 15, 2023.

   OIG Comment: Based on the DOI's response, we consider Recommendation 2 resolved but not implemented.

3. Develop and implement a process to validate the accuracy of bureau and office annual assurance statements before submitting the statements to Congress.

   DOI Response: The DOI concurred with our recommendation and stated that the OCIO will update its Annual Assurance Statement Guidance to clarify OMB and CIO requirements to provide attestations that support FISMA annual reporting. The DOI further stated that the "OCIO will also evaluate its current Annual Assurance Review Process to identify process improvements and implement them where applicable." The DOI provided a target implementation date of December 15, 2023.

   OIG Comment: Based on the DOI's response, we consider Recommendation 3 resolved but not implemented.

4. In addition to ongoing continuous monitoring, develop and implement a policy to direct system owners to test all of the controls for their systems at least every 3 years.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will clarify Departmental policy on continuous monitoring and acceptable timeframes for testing system controls based on system categorization and assessed risk." The DOI noted

that these timeframes will conform to the latest OMB and NIST guidance. The DOI provided a target implementation date of March 31, 2024.

OIG Comment: Based on the DOI's response, we consider Recommendation 4 resolved but not implemented.

5. Develop and implement a policy to ensure data and control implementation status are accurately represented in the official system of record.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will clarify Departmental policy on accurate representation of data and control implementation status in the enterprise GRC tool and provide bureaus and offices with implementation guidance." The DOI provided a target implementation date of June 30, 2024.

   OIG Comment: Based on the DOI's response, we consider Recommendation 5 resolved but not implemented.

6. Develop and implement a policy to verify that bureaus and offices perform control assessments every 3 years.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will clarify Departmental policy on control assessments and acceptable timeframes for testing system controls based on system categorization and assessed risk" and that the timeframes will conform to the latest OMB and NIST guidance. The DOI also stated that the "OCIO will evaluate functionality within the new enterprise GRC tool to determine if capabilities exist to automate a report to identify control testing dates to ensure they align with departmental policy." The DOI noted that, where this capability does not exist, the OCIO will explore establishing a customized report. The DOI provided a target implementation date of June 30, 2024.

   OIG Comment: Based on the DOI's response, we consider Recommendation 6 resolved but not implemented.

7. Develop and implement a review process that includes, at minimum, verifying that system owners have completed required testing for a sample of controls for each system before accepting the annual assurance statement.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will develop a baseline set of controls to be tested annually and will evaluate functionality within the new GRC tool to determine if capabilities exist to automate a report to notify system owners that the controls were tested within the reporting period." The DOI noted that, where this capability does not exist, the OCIO will explore establishing a customized report. The DOI provided a target implementation date of December 15, 2023.

OIG Comment: Based on the DOI's response, we consider Recommendation 7 resolved but not implemented.

8. Develop and implement a comprehensive quality control plan to perform required quarterly reviews of Plans of Action and Milestones in the official system of record to ensure that bureaus and offices address them in a timely manner, close them as appropriate, and continuously monitor and track them.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will develop a process to review POA&Ms data in the GRC tool and provide bureaus and offices with quarterly reports of pending and lapsed closure dates." The DOI further stated that it will evaluate whether the new GRC tool is capable of automating a report to alert bureaus and offices and that, where the capability does not exist, the OCIO will explore establishing a customized report. The DOI provided a target implementation date of December 15, 2023.

   OIG Comment: Based on the DOI's response, we consider Recommendation 8 resolved but not implemented.

9. Direct system owners to perform annual reviews of the data contained in all operational IT systems to ensure that an accurate privacy impact assessment has been completed and, when necessary, adjust the system's security categorization.

   DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will issue clarifying communications to reinforce the existing privacy policy and clarify the roles and responsibilities to review system data at least annually as part of the Privacy Continuous Monitoring Strategy to ensure PIAs remain accurate and to update the security categorization as necessary." The DOI provided a target implementation date of June 30, 2023.

   OIG Comment: Based on the DOI's response, we consider Recommendation 9 resolved but not implemented.

10. Develop and implement a process to ensure that a Privacy Impact Assessment is conducted before a system is granted Authorization to Operate.

    DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will issue guidance to reinforce current PIA policy and establish a process to ensure PIAs are completed for information systems before granting an ATO." The DOI provided a target implementation date of June 30, 2023.

    OIG Comment: Based on the DOI's response, we consider Recommendation 10 resolved but not implemented.

11. Develop and implement a policy clarifying the roles and responsibilities regarding control assessment and implementation.

    DOI Response: The DOI concurred with our recommendation and stated that the "OCIO will issue updated policy and supplemental guidance to further clarify and reinforce the roles and responsibilities for privacy control implementation and assessments." The DOI provided a target implementation date of June 30, 2023.

    OIG Comment: Based on the DOI's response, we consider Recommendation 11 resolved but not implemented.

Appendix 1: Scope and Methodology

Scope

We evaluated the U.S. Department of the Interior's (DOI's) information system risk management practices to determine if the DOI has appropriately authorized its systems to operate and analyzed and monitored security weaknesses to reduce the risk of compromise. Specifically, we evaluated whether the DOI authorized systems for operation based on complete and accurate risk assessments. We also evaluated remediation plans (Plans of Action and Milestones or POA&Ms) to determine whether the DOI, through its bureaus and offices, addressed and mitigated security weaknesses in a timely manner, closed the POA&Ms appropriately, and continuously monitored and tracked the plans.

Methodology

We conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work we performed provides a reasonable basis for our conclusions and recommendations.

To accomplish our evaluation objectives, we judgmentally selected a representative sample of 38 systems from the DOI's official system of record and performed the following:

- Conducted interviews with DOI, bureau, and office personnel.
- Reviewed the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology criteria.
- Evaluated DOI, bureau, and office policies and procedures related to system authorization and assessment, including POA&Ms.
- Inspected the DOI official system of record to determine whether system attributes were complete and accurate.
- Reviewed system authorizations packages for completeness and accuracy.
- Reviewed security control documentation to determine whether privacy controls were documented and assessed.
- Determined whether control assessments and quality control reviews were performed in accordance with Federal and DOI requirements.
- Reviewed prior DOI FISMA audits to determine whether systems were incorrectly excluded from annual FISMA requirements.

- Tested a sample of POA&Ms to determine whether security weaknesses were remediated completely and timely.

- Reviewed Weakness Completion Verification Forms to determine whether steps taken to address weaknesses were adequate to warrant closing the POA&M.

Appendix 2: Response to Draft Report

The U.S Department of the Interior's response to our draft report follows on page 26.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

December 22, 2022

Memorandum

To: Mark Lee Greenblatt
Inspector General

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

DARREN ASH Digitally signed by DARREN ASH
Date: 2022 12 22 15:02:59 -05'00'

From: John Clink
Acting Chief Information Security Officer
Office of the Chief Information Officer

JOHN CLINK Digitally signed by JOHN CLINK
Date: 2022 12 22 14:58:45 -05'00'

Subject: Response to Draft Report - *The U.S. Department of the Interior's Cyber Risk Management Practices Leave Its Systems at Increased Risk of Compromise* (2020-ITA-030)

Thank you for providing the Department of the Interior (Department, DOI) with the opportunity to review and comment on the draft Office of Inspector General (OIG) Report, *The U.S. Department of the Interior's Cyber Risk Management Practices Leave Its Systems at Increased Risk of Compromise (2020-ITA-030).*

We appreciate the intent and focus of this report and agree with the direction the OIG is proposing. The Department is committed to implementing requirements specified in Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, and other policies and directives that will drive our maturity in the areas identified in the report.

If you have questions, please contact John Clink, Acting Chief Information Security Officer, at [redacted].

Attachment 1: Recommendations and Responses

cc: Naznin Rahman, Chief, Audit Management Division,
Office of Financial Management
Deputy Chief Information Officers, OCIO
Chief Data Officer
Chief Technology Officer
Bureau and Office Associate Chief Information Officers
Bureau and Office Associate Chief Information Security Officers
Bureau and Office Associate Chief Data Officers
Douglas Scoville, Chief, Governance Branch, OCIO
Richard Westmark, Chief, Compliance Management Section, OCIO

Attachment 1

Management Responses to *The U.S. Department of the Interior's Cyber Risk Management Practices Leave Its Systems at Increased Risk of Compromise (2020-ITA-030)*

Recommendations and Responses

All recommendations are issued to the Department of the Interior (DOI, Department), Office of the Chief Information Officer (OCIO).

Recommendation 1: Develop and implement a process to evaluate all systems' Authorizations to Operate annually for accuracy and completeness to ensure systems are operating with a valid authorization determined by actual residual risk.

Response: Concur. The DOI OCIO will develop a process to review Authorization to Operate (ATO) data in the enterprise Governance, Risk, and Compliance (GRC) tool and alert bureaus and offices when systems are operating without valid authorization or approaching such state. The OCIO will develop customized reports in instances when the GRC tool does not natively automate generation of reports to support this process. The DOI OCIO notes that the GRC tool, which serves as the system of record, is on track to change in Fiscal Year (FY) 2023.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POC: Stacy Richkun, Cyber Risk Management Branch Chief

Target Date: December 15, 2023

Recommendation 2: Develop and implement a process to conduct quality control reviews at least annually to ensure that all systems within the official system of record (Cyber Security Assessment and Management system) have an accurate operating status.

Response: Concur. The DOI OCIO will develop a process to review ATO data in the enterprise GRC tool and alert bureaus and offices when systems have recorded a non-operational status for an extended period. The OCIO will develop customized reports in instances when the GRC tool does not natively automate generation of reports to support this process.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POC: Stacy Richkun, Cyber Risk Management Branch Chief

Target Date: December 15, 2023

Recommendation 3: Develop and implement a process to validate the accuracy of bureau and office annual assurance statements before submitting the statements to Congress.

Response: Concur. The DOI OCIO will update its Annual Assurance Statement Guidance to clarify the requirements under Office of Management and Budget (OMB) Circular A-123 Appendix D, M-18-16, and the additional Chief Information Officer (CIO) requirements to provide attestations that support the Federal Information Security Modernization Act (FISMA) annual reporting to the OMB, Department of Homeland Security (DHS), Government

Accountability Office (GAO), and specified Congressional committees. The DOI OCIO will also evaluate its current Annual Assurance Review Process to identify process improvements and implement them where applicable.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POC: Douglas Scoville, Cyber Governance Branch Chief

Target Date: December 15, 2023

Recommendation 4: In addition to ongoing continuous monitoring, develop and implement a policy to direct system owners to test all of the controls for their systems at least every 3 years.

Response: Concur. The DOI OCIO will clarify Departmental policy on continuous monitoring and acceptable timeframes for testing system controls based on system categorization and assessed risk. The timeframes will conform to the latest guidance from OMB and the National Institute for Standards and Technology (NIST).

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POC: Douglas Scoville, Cyber Governance Branch Chief

Target Date: March 31, 2024

Recommendation 5: Develop and implement a policy to ensure data and control implementation status are accurately represented in the official system of record.

Response: Concur. The DOI OCIO will clarify Departmental policy on accurate representation of data and control implementation status in the enterprise GRC tool and provide bureaus and offices with implementation guidance.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POCs: Douglas Scoville, Cyber Governance Branch Chief and Stacy Richkun, Cyber Risk Management Branch Chief

Target Date: June 30, 2024

Recommendation 6: Develop and implement a policy to verify that bureaus and offices perform control assessments every 3 years.

Response: Concur. The DOI OCIO will clarify Departmental policy on control assessments and acceptable timeframes for testing system controls based on system categorization and assessed risk. The timeframes will conform to the latest guidance from OMB and NIST. The DOI OCIO will evaluate functionality within the new enterprise GRC tool to determine if capabilities exist to automate a report to identify control testing dates to ensure they align with departmental policy. Where this capability doesn’t exist, the DOI OCIO will explore the establishment of a customized report.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POCs: Douglas Scoville, Cyber Governance Branch Chief and Stacy Richkun, Cyber Risk Management Branch Chief

Target Date: June 30, 2024

Recommendation 7: Develop and implement a review process that includes, at minimum, verifying that system owners have completed required testing for a sample of controls for each system before accepting the annual assurance statement.

Response: Concur. The DOI OCIO will develop a baseline set of controls to be tested annually and will evaluate functionality within the new enterprise GRC tool to determine if capabilities exist to automate a report to notify system owners that the controls were tested within the reporting period. Where this capability doesn't currently exist, the DOI OCIO will explore the establishment of a customized report.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POC: Stacy Richkun, Cyber Risk Management Branch Chief

Target Date: December 15, 2023

Recommendation 8: Develop and implement a comprehensive quality control plan to perform required quarterly reviews of Plans of Action and Milestones [POA&Ms] in the official system of record to ensure that bureaus and offices address them in a timely manner, close them as appropriate, and continuously monitor and track them.

Response: Concur. The DOI OCIO will develop a process to review POA&Ms data in the GRC tool and provide bureaus and offices with quarterly reports of pending and lapsed closure dates. The DOI OCIO will evaluate functionality within the new GRC tool to determine if capabilities exist to automate a report to alert bureaus and offices. Where this capability doesn't currently exist, the DOI OCIO will explore the establishment of a customized report.

Responsible Official: John Clink, Acting Chief Information Security Officer
OCIO POC: Stacy Richkun, Cyber Risk Management Branch Chief

Target Date: December 15, 2023

Recommendation 9: Direct system owners to perform annual reviews of the data contained in all operational IT systems to ensure that an accurate privacy impact assessment has been completed and, when necessary, adjust the system's security categorization.

Response: Concur. Department policy requires system owners to monitor privacy impact assessments (PIAs) and privacy risks at the system and information level through its life cycle as part of the DOI Privacy Continuous Monitoring Strategy and to review PIAs at least annually or when a trigger event occurs that has privacy implications or creates privacy risk. The DOI OCIO will issue clarifying communications to reinforce the existing privacy policy and clarify the roles and responsibilities to review system data at least annually as part of the Privacy Continuous

Monitoring Strategy to ensure PIAs remain accurate and to update the security categorization as necessary.

Responsible Officials: John Clink, Acting Chief Information Security Officer and Teri Barnett, Departmental Privacy Officer

Target Date: June 30, 2023

Recommendation 10: Develop and implement a process to ensure that a Privacy Impact Assessment is conducted before a system is granted Authorization to Operate.

Response: Concur. The DOI PIA Guide and Privacy Control Standards require a completed PIA that is approved by the Senior Agency Official for Privacy (SAOP) before a system is granted an ATO. The DOI OCIO will issue guidance to reinforce current PIA policy and establish a process to ensure PIAs are completed for information systems before granting an ATO.

Responsible Officials: John Clink, Acting Chief Information Security Officer and Teri Barnett, Departmental Privacy Officer

Target Date: June 30, 2023

Recommendation 11: Develop and implement a policy clarifying the roles and responsibilities regarding control assessment and implementation.

Response: Concur. Current DOI policy outlines roles and responsibilities for privacy control implementation, assessment, and monitoring. The DOI OCIO will issue updated policy and supplemental guidance to further clarify and reinforce the roles and responsibilities for privacy control implementation and assessments.

Responsible Officials: John Clink, Acting Chief Information Security Officer and Teri Barnett, Departmental Privacy Officer

Target Date: June 30, 2023

Appendix 3: Status of Recommendations

Recommendation	Status	Action Required
1–11	Resolved but not implemented	We will refer these recommendations to the Office of Policy, Management and Budget to track implementation.

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

REPORT FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

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

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

Who Can Report?

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

How Does it Help?

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

Who Is Protected?

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