Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Security Assessment and Authorization Process

A-14-21-51093 September 2024

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 25, 2024 **Refer to:** A-14-21-51093

To: Martin O’Malley
Commissioner

From: Michelle L. Anderson Michelle L Anderson
Assistant Inspector General for Audit
as Acting Inspector General

Subject: Security Assessment and Authorization Process

The attached final report presents the results of the Office of Audit’s review. The objective was to determine whether the Social Security Administration was managing its Security Assessment and Authorization process in accordance with Federal and Agency requirements.

If you wish to discuss the final report, please contact Jeffrey Brown,
Deputy Assistant Inspector General for Audit.

Attachment

Security Assessment and Authorization Process
A-14-21-51093

September 2024 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration (SSA) was managing its Security Assessment and Authorization (SA&A) process in accordance with Federal and Agency requirements.

Background

The *Federal Information Security Modernization Act of 2014* and Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, require that all Federal agencies institute an agency wide program to secure the information and systems that support their operations and assets, and implement the Risk Management Framework described in National Institute of Standards and Technology Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

SSA's Division of Compliance and Assessments oversees the Agency's SA&A and risk management processes. It monitors the Agency's existing systems, tests selected security controls, and assesses systems every 3 years or when major changes are made. Before SSA releases a new, or significantly revised existing, information system into production, system owners must conduct an SA&A to ensure the information system is operating under an acceptable level of risk and obtain/renew an Authority to Operate.

Results

SSA was managing the following aspects of its SA&A process in accordance with Federal and Agency requirements:

- System owners identified the missions, business functions, and mission/business processes each system was intended to support; the types of information the system was to process, store, and transmit; and all stages of the information life cycle for each information type the system processed, stored, or transmitted.
- The Agency selected the appropriate assessor, who achieved the appropriate level of independence. Additionally, system owners provided the assessor the documentation they needed to conduct the assessments.

However, SSA was not managing the following aspects of its SA&A process in accordance with Federal and Agency requirements:

- The Agency did not apply updated security and privacy controls and had not implemented privacy requirements.
- The Agency had not performed an Agency-level risk assessment, and system owners were not conducting system-level risk assessments.
- The organization-wide continuous monitoring strategy did not identify the required information and had not been approved by a senior Agency official.
- Some Agency personnel did not follow Agency policies and procedures.
- Agency policy and processes did not include the level of detail necessary to ensure stakeholders were aware of their responsibilities.

Recommendations

We made 19 recommendations to help ensure SSA manages its SA&A process in accordance with Federal and Agency requirements.

Agency Comments

SSA agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

FedRAMP	Federal Risk and Authorization Management Program
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIRA	Privacy Impact and Risk Assessment
POA&M	Plan of Actions and Milestones
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SSA	Social Security Administration
SP	Special Publication

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) was managing its Security Assessment and Authorization (SA&A) process in accordance with Federal and Agency requirements.

BACKGROUND

The Federal Information Security Modernization Act of 2014 requires that all Federal agencies institute an agency-wide program to secure the information and systems that support their operations and assets.[1] Additionally, Office of Management and Budget (OMB) Circular A-130[2] requires that agencies implement the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF).[3]

NIST describes Federal agencies' mandatory use of the RMF and "provides guidelines for applying the RMF to information systems and organizations. The RMF provides 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."[4] The RMF provides a flexible, holistic, and repeatable process and links to a suite of NIST standards and guidelines that help programs meet Federal requirements.[5] This is an iterative process. After completing the RMF steps, entities must continually monitor the controls.

When SSA's Chief Information Officer authorizes a system to operate, it accepts the risks the system may pose to Agency operations, assets, or individuals based on a documented set of security controls. Without a complete SA&A program, the Agency increases the possibility that:

1. it will not identify weaknesses in the system controls or whether it should authorize a system to operate and
2. the authorizing official could accept unknown exploitable risks that could result in data loss or breach and will be unaware of system changes that may be significant.

SSA's Division of Compliance and Assessments oversees the Agency's SA&A and risk management processes, monitors existing systems, tests selected security controls, and assesses systems every 3 years or when major changes are made. Before SSA releases a new, or significantly revised existing, information system into production, system owners must conduct an SA&A to ensure the information system is operating under an acceptable level of risk and obtain/renew an Authority to Operate from the Agency's Chief Information Officer.

[1] *Federal Information Security Modernization Act of 2014,* 44 U.S.C. §§ 3551 through 3559.

[2] OMB, *Managing Information as a Strategic Resource,* Circular A-130, Appendix I, sec. 5.a, p. I-16 (July 28, 2016).

[3] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2* (December 2018).

[4] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. ii (December 2018).

[5] *Federal Information Security Modernization Act of 2014,* 44 U.S.C. §§ 3551 through 3559.

Scope and Methodology

To achieve our objective, we reviewed Federal requirements and SSA policies, procedures, and internal control documentation. We also interviewed Agency personnel responsible for the SA&A process. We reviewed documentation for a sample of 18 information systems to determine whether Federal guidance and Agency policies and procedures were followed. See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

SSA was managing the following aspects of its SA&A process in accordance with Federal and Agency requirements:

- System owners:
  - identified the missions, business functions, and mission/business processes each system is intended to support;
  - determined the system's authorization boundary;[6]
  - identified the types of information the system was to process, store, and transmit; and
  - identified all stages of the information life cycle for each information type the system processed, stored, or transmitted.
- The Agency selected the appropriate assessor who achieved the appropriate level of independence. Additionally, system owners provided the assessor the documentation they needed to conduct the assessments.

However, SSA was not managing the following aspects of its SA&A process in accordance with Federal and Agency requirements:

- The Agency did not apply updated security and privacy controls.
- The Agency had not implemented privacy requirements.[7]
- The Agency had not identified and assigned a senior accountable official for risk management.
- The Agency had not performed an Agency-level risk assessment, and system owners were not conducting system-level risk assessments.
- The organization-wide continuous monitoring strategy did not identify the required information and had not been approved by a senior Agency official.

[6] The authorization boundary includes all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the information system is connected. OMB, *Managing Information as a Strategic Resource,* Circular A-130, sec. 10.a.7 p.27 (July 28, 2016).

[7] In 2022, we reported similar issues in an audit that found the system Agency staff used to manage the enumeration workload during the pandemic did not have all the required security and privacy assessments before implementation. SSA completed these required activities in January 2023. SSA, OIG, *SSA's Enumeration Services During the COVID-19 Pandemic, A-15-21-51015*, p. 19 (September 2022).

- Some Agency personnel did not follow Agency policies and procedures.
- Agency policy and processes did not include the level of detail necessary to ensure stakeholders were aware of their responsibilities.

Federal Guidelines/Requirements

NIST standards and guidelines associate each information system with an impact level.[8] "The standards and guidelines also provide a corresponding . . . baseline security controls and tailoring guidance to ensure the security controls in the approved information system security plan . . . and controls in the privacy plan . . . satisfy the information security, privacy, and mission or business protection needs of the agency."[9]

Security and Privacy Controls

OMB requires that Federal agencies comply with new or updated material in NIST standards and guidelines within 1 year of their publication dates unless otherwise directed by OMB.[10] Additionally, NIST requires that system owners select "controls for the system and the environment of operation."[11] NIST designed security and privacy controls to protect systems and the information they contain commensurate with the risk associated with their misuse or unauthorized disclosure. Similar controls are grouped into 20 families of security and privacy controls related to a specific topic that may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms. NIST added two control families—personally identifiable information processing and transparency controls and supply chain risk management controls[12]—when NIST updated SP 800-53 in September 2020.[13] SSA had not selected, designed, or implemented these two control families. SSA should have complied with the updated guidance by December 2021.

[8] An impact level is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. NIST, *Guide for Conducting Risk Assessments*, *800-30 Rev 1*, p. B-5 (December 2018).

[9] OMB, *Managing Information as a Strategic Resource*, Circular A-130, Appendix I, sec. 5.a, p. I-16 (July 28, 2016).

[10] For legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within 1 year of their respective publication dates unless otherwise directed by OMB. OMB, *Managing Information as a Strategic Resource*, Circular A-130, Appendix I, sec. 5.a p. I-16 (July 28, 2016).

[11] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 50 (December 2018).

[12] The personally identifiable information processing and transparency controls address privacy risk management. The supply chain risk management controls leverage and expand on supply chain threats to the information system.

[13] NIST SP 800-53, Revision 5, which supersedes Revision 4, made "more than editorial or administrative change[s]" to 698 controls and control enhancements including the addition of 268 new controls and control enhancements, and withdrawal of 90 controls and control enhancements. NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, *SP 800-53 Rev. 5* (September 2020, amended December 2020).

SSA was transitioning to the most recent NIST security and privacy controls and had not identified the security and privacy controls needed to manage risk and satisfy all Federal security and privacy requirements.[14] In February 2023, SSA's Chief Information Security Officer signed a Risk Acceptance stating, "SSA has reviewed the risk of not assessing against the full set of Rev[ision] 5 control, and the specific controls not yet being assessed for SSA systems represent areas of lower risk with respect to our mission/business needs." However, the Risk Acceptance was not in place during the entirety of our audit.

In May 2023, the General Services Administration released baseline for Cloud Service Providers based on NIST 800-53, Revision 5. SSA has a large cloud presence that depends on the Federal Risk and Authorization Management Program (FedRAMP) framework. SSA was waiting for the release of the NIST 800-53, Revision 5 FedRAMP baseline and the updated Customer Responsibility Matrix from the Cloud Service Providers. Additionally, there was a technical complication with SSA's risk-management software when it migrated the NIST 800-53 Revisions. Essentially, two projects would co-exist in SSA's risk management software: one for Revision 4 and one for Revision 5. Fulfilling the requirements of these Revisions would result in SSA duplicating all work required to maintain every information system in its risk management software.

The unimplemented security and privacy controls undermine SSA's ability to protect information systems and their contents from unauthorized access, use, disclosure, disruption, modification, or destruction, to help provide confidentiality and integrity while maintaining data availability.

Privacy Requirements

OMB requires that Federal agencies ". . . [d]evelop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls."[15] These plans establish the security and privacy controls selected for implementation and form the basis for a system authorization. The privacy plan and system security plan may be integrated into one consolidated document.[16] Agencies are also required to conduct[17] and

[14] *Federal Information Security Modernization Act of 2014,* 44 U.S.C. §§ 3551-3559; the *Privacy Act of 1974*, 5 U.S.C. § 552a; selected OMB policies (for example, OMB Circular A-130); and designated Federal Information Processing Standards that are incorporated in NIST SP 800-53.

[15] OMB, *Managing Information as a Strategic Resource, Circular A-130,* Appendix I, sec. 4.c.9, p. I-6 (July 28, 2016).

[16] The consolidated document ". . . details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls." OMB, *Managing Information as a Strategic Resource, Circular A-130,* sec. 10.e.65, p. 34 (July 28, 2016).

[17] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 64 (December 2018).

document privacy control assessments[18] "prior to the operation of an information system, and periodically thereafter."[19]

The system owners did not complete Privacy Plans and Privacy Assessment Plans for any of our sampled systems,[20] and the control assessors did not have what they needed to complete Privacy Assessment Reports. The Agency requires that system owners complete Privacy Impact and Risk Assessments for systems undergoing an authorization decision. SSA provided Privacy Impact and Risk Assessments for some of our sampled systems.[21] However, the documents did not include:

- privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks;
- details on how the controls had been implemented; and
- methodologies and metrics that would be used to assess the controls.

Because SSA is in the final stages of implementing the privacy requirements in NIST SP 800-53, Revision 5 guidelines, the Agency does not require that system owners complete Privacy Plans, Privacy Assessment Plans, and Privacy Assessment Reports.[22] Without documented Privacy Plans, the Agency's privacy requirements may not be satisfied and managed, and the Agency may not be able to ensure compliance with applicable privacy requirements. Additionally, the privacy of individuals may not be protected.

Documentation

The National Archives and Records Administration (NARA) requires that records be maintained until 1 year after a system is superseded by a new iteration or when the records are no longer needed for agency purposes.[23] Additionally, NARA states "Federal employees are responsible for making and keeping records of their work," which includes taking ". . . care of records so that information can be found when needed" and "setting up good directories and files and filing materials (in whatever format) regularly and carefully in a manner that allows them to be safely stored and efficiently retrieved when necessary."[24]

[18] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 65 (December 2018).

[19] OMB, *Managing Information as a Strategic Resource, Circular A-130,* Appendix I, sec. 4.c.14, p. I-6 (July 28, 2016).

[20] Refer to Appendix A for descriptions of the sampled systems.

[21] For more information regarding the Privacy Impact and Risk Assessments, refer to *Agency Policies/Procedures.*

[22] Revision 5 included 96 privacy control baseline for federal agencies to address privacy requirements and manage privacy risks that arise from the processing of personally identifiable information.

[23] National Archives and Records Administration (NARA), *General Records Schedule 3.2: Information Systems Security Records*, Item 010 (January 2023).

[24] NARA, *National Archives - Federal Records Management*, Frequently Asked Questions about Records Management in General, archives.gov (July 11, 2017).

SSA could not provide all documentation for 1 system to support testing related to 27 tasks in NIST SP 800-37.[25] Missing documentation included, but was not limited to, System Security Plans, Security Assessment Plans and Reports, and an Authorization to Operate. According to SSA, these documents were not available to Agency personnel because, during a 2017 reorganization, the records were not transferred to the new component. Without documentation, the Agency cannot verify it implemented the system security and privacy controls or ensure ongoing monitoring of those systems. Therefore, the Agency could have systems in its environment that could be at risk because the security and privacy controls were not implemented.

Risk Management Framework

There are seven steps in the RMF.[26] Until December 2022, SSA's SA&A process included six of the RMF's seven steps. In December 2022, SSA updated its policy to include the Prepare step and accurately reflect all seven steps of the RMF.[27]

1. Prepare
2. Categorization of Information and Information Systems
3. Select Security Controls
4. Implement Security Controls
5. Assess Security Controls
6. Authorize Information Systems
7. Continuous Monitoring

All seven steps are essential for the RMF's successful execution. The RMF defines essential activities that personnel at all levels should know to manage security and privacy risks. This includes identifying and assigning key risk management roles, establishing a risk management strategy, and assessing organization-wide security and privacy risks.

[25] Refer to Appendix A for more information regarding systems sampled and Appendix B for more information regarding the 47 Risk Management Framework tasks.

[26] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 8 (December 2018).

[27] Part of the *Prepare* step is asset identification. While not noted here, an issue was identified in the audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2023. Specifically, SSA needed to fully implement its policies and processes for maintaining a complete and accurate inventory of information systems, hardware, and software. SSA, OIG, *Summary of the Audit of the Social Security Administration's Information Security Program and Practices for Fiscal Year 2023, 142306*, p. 6 (September 2023).

Senior Accountable Official for Risk Management

NIST requires that the head of the Federal agency identify and assign individuals to specific roles associated with security and privacy risk management.[28] This includes the senior accountable official for risk management, who ". . . leads and manages the risk executive (function) in an organization and is responsible for aligning information security and privacy risk management processes with strategic, operational, and budgetary planning processes. The senior accountable official for risk management is the head of the agency or an individual designated by the head of the agency."[29]

However, SSA's senior management did not designate someone to be the senior accountable official for risk management and did not establish the necessary requirements in the Risk Management Strategy.[30] SSA cannot ensure system owners are (1) addressing security and privacy risk management processes and (2) following the Agency's strategic, operational, and budgetary planning processes.

Risk Management Strategy

NIST requires that the Agency establish a risk management strategy that makes explicit the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investments and operational decisions.[31] The strategy should include the strategic-level decisions and considerations for how senior leaders and executives are to manage security and privacy risks. The risk management strategy should also include the organizational risk tolerance; acceptable risk assessment methodologies and risk response strategies; a process for consistently evaluating security and privacy risks organization-wide; and approaches for monitoring risk over time.

Although the Agency has established a Cybersecurity Risk Management Strategy, SSA's senior management did not establish the necessary requirements in the Agency Risk Management Strategy including the organizational risk tolerance and did not make explicit the threats, assumptions, constraints, and trade-offs used for making investment and operational decisions. If the Agency does not establish its risk tolerance, it may unintentionally accept risk it cannot tolerate.

[28] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 29 (December 2018).

[29] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, Appendix D, p. 121 (December 2018).

[30] SSA's Chief Information Security Officer is the Agency's Cybersecurity Risk Executive but is not responsible for the entirety of the Agency's Risk Management process.

[31] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 29 (December 2018).

Risk Assessments

The Agency must complete or update an organization-wide risk assessment on an ongoing basis.[32] Additionally, NIST requires that system owners conduct a system-level risk assessment and update the risk assessment results continually.[33] Risk assessments at the organizational level leverage aggregated information from system-level risk assessment results, continuous monitoring, and any strategic risk considerations relevant to the organization. "The organization considers the totality of risk from the operation and use of its information systems, from information exchange and connections with other internally and externally owned systems, and from the use of external providers."[34]

System-level risk assessments include security and privacy risk assessments. However, as of the date of our review, SSA had not conducted an Agency-level risk assessment, and system owners were not conducting system-level risk assessments. Although the Agency completed an Agencywide Cybersecurity Risk Assessment in February 2024, risk assessments should not be limited to cyber-security risks. The Agency's risk-management policies did not include organizational risk assessments or system-level risk assessments. Therefore, the Agency may not be able to ensure each type of risk is fully assessed or identify threat source. In addition, there is increased likelihood an asset's vulnerability will be exploited by a threat that could result in the asset's loss. Finally, the Agency cannot use risk-assessment results to inform categorization decisions; the selection, tailoring, implementation, and assessment of controls; authorization decisions; and potential courses of action and prioritization for risk responses.

Continuous Monitoring Strategy

NIST requires the development and implementation of an organization-wide strategy for monitoring control effectiveness that identifies

> . . . the minimum monitoring frequency for implemented controls across the organization; defines the ongoing control assessment approach; and describes how ongoing assessments are to be conducted (e.g., addressing the use and management of automated tools, and instructions for ongoing assessment of controls for which monitoring cannot be automated).[35]

The continuous monitoring strategy may also define security and privacy reporting requirements including who receives the reports. The senior accountable official for risk management or the risk executive (function) approves the continuous monitoring strategy including the minimum frequency with which controls are to be monitored.

[32] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 30 (December 2018).

[33] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 41 (December 2018).

[34] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 30 (December 2018).

[35] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 34 and 35 (December 2018).

SSA's organization-wide continuous monitoring strategy does not include information (or reference other Agency instructions) to:

1. identify minimum monitoring frequency for implemented controls across the organization;

2. define the ongoing control assessment approach; or

3. describe how ongoing assessments are to be conducted.

Additionally, the appropriate SSA official had not approved the strategy.

SSA has defined the continuous monitoring elements on separate pages of its internal websites; however, the continuous monitoring strategy did not refer to these items. Therefore, the Agency and stakeholders could not efficiently and cost-effectively monitor the effectiveness of controls implemented within, or inherited by, organizational systems, which is an important aspect of risk management. Maintaining ongoing awareness of information security, vulnerabilities, and threats supports organizational risk-management decisions. Additionally, because the items are not linked to the Strategy, stakeholders may not be aware of the items and their responsibilities, and these parts of the Strategy might not get updated timely.

Agency-specific Requirements

SSA developed an information security policy to protect the Agency's information technology resources and data as well as manage risk in a secure environment. All personnel acting on the Agency's behalf and use its information systems must follow the security policy. Additionally, SSA had developed standard operating procedures that provide stakeholders with step-by-step instructions and process information as well as clear and concise instructions on how to properly function within SSA's risk management software.

Agency Policies/Procedures

We noted Agency personnel were not following all Agency policies and procedures.

1. **Plans of Action and Milestone (POA&M).** SSA requires that security authorization managers create a POA&M no later than 10 business days after the final Security Assessment Report is delivered. For six systems, security authorization managers did not create a POA&M for each risk identified in the Security Assessment Report. As a result, the authorizing official and other related parties will not be able to review and agree on the remediation actions planned to correct the identified deficiencies as well as the direct/indirect effect the deficiencies may have on the system's security and privacy posture and the organization's risk exposure and therefore cannot monitor progress in completing the actions.

2. **Business Impact Analysis.** SSA requires that the security authorization manager develop security documentation, including the System Security Plan, Information Security Contingency Plan, and the Business Impact Analysis. For three systems, a Business Impact Analysis was provided; however it was not signed by the appropriate personnel. For one system, an Information Security Contingency Plan was not provided. Outdated and incomplete documentation may not identify risks that affect the system and potentially hinder the quick and effective recovery of systems following a disruption. Additionally, system owners may not be aware of contingency roles and responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure.

3. **Privacy Impact and Risk Assessment (PIRA).** A PIRA must be performed for information systems or applications seeking an Authorization to Operate. Additionally, the security authorization manager and Senior Agency Official for Privacy must approve PIRAs. We found the appropriate stakeholders did not sign the PIRA for two systems, evidence of a PIRA was not provided for three systems, and a PIRA was not conducted for three systems. Privacy compliance requirements or privacy risks may not be identified.

4. **Authority to Operate.** OMB requires that Federal agencies authorize an information system before it is authorized and made operational and periodically thereafter.[36] SSA requires that all information technology assets be included in an information system boundary and covered by that boundary's authorization. However, SSA did not provide evidence for two sampled systems that were authorized before they went into production, and it could not provide evidence of an authorization for two other systems. If SSA's authorizing official does not issue an Authorization to Operate for all its systems, SSA may not be able to verify what activities system owners completed to protect against security and privacy risks to the Agency's operations and assets and whether the risks are acceptable to the authorizing official.

5. **FedRAMP.** When using a Cloud Service Provider, SSA requires that security authorization managers select a FedRAMP authorized cloud offering. However, for two systems, a FedRAMP-authorized cloud offering was not selected. SSA and system owners could be putting the Agency at risk for fines or other noncompliance consequences.

6. **Risk Briefing.** The Office of Information Security completes a risk briefing for each system to gain an Authorization to Operate. However, a risk briefing was not provided for one system. Agency personnel may not be aware of the system's risk posture.

7. **Continuous Monitoring.** SSA requires that the security authorization manager attend cloud-service provider continuous-monitoring meetings (if available), or, at minimum, review continuous-monitoring reports to remain aware of new risks and remediation activities. The security authorization manager for one sampled system did not attend these meetings or review the reports as required. SSA personnel may not be aware of risks and remediation activities by the Cloud Service Provider and the risk exposure to the Agency operations.

[36] OMB, *Managing Information as a Strategic Resource, Circular A-130,* Appendix I, sec. 4.d.2, p. I-6 (July 28, 2016).

8. **System Security Plans.** SSA policy requires that the security authorization manager be responsible for writing and maintaining the security plan for the system, and the system owner be accountable for ensuring the plan is maintained and current. However, the system owner did not assign required security controls for five sampled systems. In addition, the system owner did not document control implementation and tailoring actions for two sampled systems. Without this documentation, SSA may not allocate or implement controls or allocate or implement them within its policy. This could make the Agency vulnerable to security and privacy risks.

Agency Policy

NIST requires that system owners:

- Develop a continuous monitoring strategy that reflects the organizational risk-management strategy.[37]
- Monitor changes that affect the system's security and privacy posture,[38] analyze the continuous monitoring activities' output,[39] and update the risk-management documents based on continuous monitoring activities.[40]
- Report the security and privacy posture to the authorizing official and other senior leaders and executives.[41]

However, Agency policy did not require that system owners (1) develop a system-level continuous monitoring strategy; (2) monitor changes; (3) analyze the output continuous monitoring activities, and update documents based on the activities; and (4) report the security and privacy posture to the authorizing official or other senior leaders.

SSA cannot monitor controls if they are not provided as part of the Agency-level continuous monitoring strategy, which can create a lack of assurance the controls are working as designed. Also, the authorizing official and other officials may not know of real-time changes and concerns in the security and privacy posture for Agency systems.

[37] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 55 (December 2018).

[38] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 76 and 77 (December 2018).

[39] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 78 and 79 (December 2018).

[40] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 79 (December 2018).

[41] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 80 (December 2018).

Agency Process

SSA information systems must incorporate the RMF, as required by OMB.[42] However, the Agency did not have a more detailed process that required system owners document specific items as noted below. Additionally, personnel may be assigned as a "designated representative," but the assignment of that role is not documented in Agency procedures. We noted:

1. **Security and Privacy Plans.** The authorizing official (or designated representative) must review and approve the security and privacy plans.[43] However, evidence did not show the authorizing official or designated representative had reviewed and approved the security plan. SSA system owners or security authorization managers must review, update, and approve all security documentation annually or as major changes occur to ensure accuracy. However, neither the system owner nor the security authorization manager were the authorizing official's designated representative. Plans may not be complete, consistent, and satisfy the stated security and privacy requirements for the system. The authorizing official or designated representative may recommend changes to the security and privacy plans. If the plans are unacceptable, the system owner may have to make appropriate changes to the plans.

2. **Risk Determinations.** The authorizing official (or designated representative) should determine the risk of operating or using the system.[44] The authorizing official did not make risk determinations for the 18 systems we sampled. Per Agency personnel, the signed Authorization to Operate is the risk determination. Without a risk determination, personnel may not have analyzed system risks and accurately responded to the risk.

3. **Ongoing Authorizations.** NIST requires that authorizing officials continually review the system's security and privacy posture to determine whether the risk remains acceptable.[45] To employ an ongoing authorization approach, organizations must have an organization- and system-level continuous monitoring process in place to assess implemented controls. However, SSA did not have a process that required the authorizing official conduct ongoing authorization of information systems.[46] The authorizing official and other officials may not be aware of changes in the security and privacy posture for Agency systems.

[42] OMB, *Managing Information as a Strategic Resource, Circular A-130,* Appendix I, sec. 3.b.5, p. I-2 (July 28, 2016).

[43] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 56 (December 2018).

[44] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 71 (December 2018).

[45] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 81 and 82 (December 2018).

[46] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 139 and140 (December 2018). The authorizing official is provided the necessary information regarding the system's near real-time security and privacy posture to determine whether the mission/business risk of continued system operation or the common controls provision is acceptable. Ongoing authorization is fundamentally related to the ongoing understanding and ongoing acceptance of security and privacy risk and is dependent on a robust continuous monitoring program.

4. **System Owner Requirements.** System owners are required to identify the stakeholders having an interest in the system,[47] identify and prioritize stakeholder assets,[48] and allocate the security and privacy requirements to the system and the environment in which the system operates.[49] The system owners did not identify or document these items. The Agency may not be able to carry out essential activities at the organization, mission and business processes, and information system levels to help prepare the organization to manage its security and privacy risks.

5. **Security Assessment Plan Approvals.** The authorizing official, or designated representative, reviews the security categorization results and decisions[50] and reviews and approves the security and privacy assessment plans to establish the expectations for the control assessments and the level of effort required.[51] SSA could not provide evidence that showed the authorizing official, or a designated representative, reviewed and approved the security categorization and security assessment plans. The authorizing official may not be able to ensure the security documentation is consistent with the organization's mission and business functions, the need to adequately protect those missions and functions, and security and privacy objectives of the organization.

6. **Control Assessment Recommendations.** Control assessors are required to prepare assessment reports that document the findings and recommendations from the control assessments.[52] The Security Assessment Reports included the findings identified during the assessment but not recommendations. Therefore, SSA may not be able to determine the risk to organizational operations and assets, individuals, and other organizations.

CONCLUSION

Without an SA&A program that complies with Federal requirements, the Agency increases the possibility that:

- information system-related security and privacy risk are not being adequately addressed;
- it will not identify weaknesses in the system privacy controls or when determining whether it should authorize a system to operate; and

[47] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 37 (December 2018).

[48] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 38 (December 2018).

[49] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 44 (December 2018).

[50] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 48 and 49 (December 2018).

[51] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 61 (December 2018).

[52] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, pp. 65 and 66 (December 2018).

- the authorizing official may not be aware of or understand the risk associated with operating the information system and unknowingly accept exploitable risks that could result in data loss or breach, and the authorizing official will be unaware of system changes that may be significant.

RECOMMENDATIONS

We recommend SSA:

1. Complete the implementation of NIST SP 800-53, Revision 5.
2. Update policies and procedures to require that system owners define the privacy requirements for the system and the environment of operation, including where those requirements should be documented.
3. Remind Agency personnel of NARA regulations.
4. Identify and assign the senior accountable official for risk management.
5. Include the organizational risk tolerance and make explicit the threats, assumptions, constraints, and trade-offs used for making investment and operational decisions in the Risk Management Strategy.
6. Document and implement procedures for conducting and updating an organization- and system-level risk assessment.
7. Update the information security continuous monitoring strategy to include the monitoring requirements at the mission/business process and information system levels; the minimum monitoring frequency for implemented controls across the organization; and how ongoing assessments are to be conducted.
8. Update policies and procedures to require that the senior accountable official for risk management, or other designated official, review and approve the continuous monitoring strategy and retain evidence of the review and approval.
9. Remind Agency personnel of policies and procedures, including compliance with roles and responsibilities noted in policy, and updating the security plan to document appropriate security control allocations and control tailoring.
10. Centralize policies and procedures related to the SA&A process.
11. Update Agency policy to comply with Federal regulations for SA&A. Specifically, complete a system-level continuous monitoring strategy.
12. Update Agency policy to comply with Federal regulations for SA&A. Specifically, require that system owners review and update Security Assessment Reports, System Security Plans, and POA&Ms based on the results of the continuous monitoring process.

13. Update Agency policy to comply with Federal regulations for SA&A. Specifically, require that system owners report the security and privacy posture of the system to the authorizing and other organizational officials and define how often these updates should happen.

14. Update Agency process documentation, as applicable, to establish a process to document the review and approval of system security and privacy plan by the authorizing official or designated representative.

15. Update Agency process documentation, as applicable, to designate the signed Authorization to Operate is the risk determination completed by the authorizing official or a designated representative.

16. Update Agency process documentation, as applicable, to require that the authorizing official review systems' security and privacy posture on an ongoing basis.

17. Update Agency process documentation, as applicable, to require that system owners identify, define, and document requirements from the *Prepare* phase.

18. Update Agency process documentation, as applicable, to establish a process to document the review and approval of Security Categorization and Security Assessment Plan by the authorizing official or designated representative.

19. Update Agency process documentation, as applicable, to establish a process to include recommendations in all future Security Assessment Reports.

AGENCY COMMENTS

SSA agreed with our recommendations. See Appendix C for the full text of SSA's comments.

OTHER MATTERS

Before we conducted this audit, SSA established a security authorization manager and system owner for regional applications, analyzed critical applications, and developed system boundaries. However, it took time for the Agency to develop the security documentation for those boundaries. So it created the Regional Application Boundary to provide a provisional authorization for all critical regional applications while each one went through the SA&A process. The Regional Application Boundary did have an Authorization to Operate but did not have all the security documentation. During our audit, SSA decommissioned the Regional Application Boundary and broke it out into other boundaries. Since the Boundary is no longer in use, we are not including any issues identified for it in this report.

Additionally, for other systems throughout SSA, we noted system owners and security authorization managers were not centralized within the Office of the Chief Information Officer. Because of this decentralization, there is a lack of oversight to ensure system owners and security authorization managers meet federal requirements. Although we are not issuing a formal recommendation for centralizing system owners and security authorization managers, we are bringing this to the attention of stakeholders.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objectives, we:

- Reviewed applicable Federal regulations and guidance related to the Security Assessment and Authorization (SA&A) process, including the following:
  - Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016) and
  - National Institute of Standards and Technology (NIST) *Risk Management Framework for Information Systems and Organization: A System Life Cycle Approach for Security and Privacy*; *Special Publication 800-37* (December 2018).
- Reviewed the Social Security Administration's (SSA) policies and procedures pertaining to the SA&A process including, but not limited to:
  - SSA's Information Security Policy;
  - the *Information Security Continuous Monitoring* internal website; and
  - the *Establishing an Authorization to Operate* internal website.
- Selected a non-statistical sample of 18 information systems.

Table A–1: Sampled Systems

Sample Number	System Description
1	The Infrastructure as a Service environment necessary to support SSA platforms, applications, and development operations deployments in the cloud.
2	A common control provider that supplies the baseline configuration policy and security controls as a service.
3	Offers secure and private authentication of users accessing the Agency's online *my* Social Security account through a centralized single platform Federated Identity System.
4	Used to manage the scanners, the content library, scanning configurations, and scheduled scan jobs.
5	A secure and scalable software as a service for your geospatial workflows.
6	Provides automated case management in support of special tax circumstances when U.S. citizens are temporarily working abroad.
7	Encompasses the activities associated with taking applications for Social Security benefits, determining entitlement and eligibility, establishing records of entitlement, and interfacing the results of processing with other payments.
8	Optimizes sorting multiple mailing jobs through collating and pre-sorting multiple print jobs before they are printed, among other functions.
9	The current standardized server platform and environment of operation for the Office of Central Operation applications.
10	Used to collect and process Social Security number applications.

Sample Number	System Description
11	Informs the public of the Office of the Inspector General's (OIG) statutory mission to promote economy, efficiency, and effectiveness in the administration of SSA programs and operations; OIG's efforts to prevent and detect fraud, waste, abuse; and how they can report suspected fraud, waste, and abuse.
12	Provides a high-performance electronic statement retrieval and enterprise report management solution and captures the print image of program notices and other documents.
13	The common control provider project for Enterprise Architecture.
14	Provides access to SSA Net through a multi-layered infrastructure servers.
15	Provides for the use of major earning files and data for individuals and employers.
16	Handles a broad array of disability case processing and associated functionality such as case processing/adjudication, reconsideration/appeals processing, and fiscal processing.
17	Allows permitted entities to verify if an individual's Social Security number, name, and date of birth combination matches Social Security records.
18	Used to maintain the business mission of the regions, while reorganizing the system boundaries to incorporate increased ownership of applications by their appropriate region.

- Reviewed supporting documentation for each sampled information system, including the:
  - System Security Plan;
  - Security Assessment Report;
  - Plan of Actions and Milestones;
  - Authorization to Operate; and
  - Enterprise Architecture Approval.
- Interviewed SSA personnel responsible for the SA&A process and Agency policies.
- Verified Agency policies and procedures were being followed.

We conducted our audit from March 2022 through April 2024. The principal entity reviewed was the Division of Compliance and Assessments within the Office of Information Security under the Office of the Chief Information Officer.

We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components, including control environment, risk assessment, control activities, information and communication, and monitoring. In addition, we reviewed the principles of internal controls associated with the audit objective. We identified the following components and principles as significant to the audit objective.

- Component 2: Risk Assessment
    - Principle 6 - Define objectives and risk tolerances
    - Principle 7 - Identify, analyze, and respond to risk
    - Principle 9 - Analyze and respond to change
- Component 3: Control Activities
    - Principle 11 - Design activities for the information system
- Component 4: Information and Communication
    - Principle 13 - Use quality information
- Component 5: Monitoring
    - Principle 16 - Perform monitoring activities

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B – Risk Management Framework Tasks and Related Findings

The National Institute of Standards and Technology's (NIST) risk management framework provides guidance for managing risk throughout information system design, development, implementation, operation, and disposal, and in the environments in which those systems operate[1] and the correlating findings.

Step 1: Prepare

The Prepare step carries out essential activities at the organization, mission and business process, and the organization's information system levels to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.[2]

Table B–1: Prepare Tasks

Risk Management Task Number	Task Description	Related Finding
P-1: Risk Management Roles	Identify and assign individuals to specific roles associated with security- and privacy-risk management.	Senior Accountable Official for Risk Management
P-2: Risk Management Strategy	Establish a risk-management strategy for the organization that includes a determination of risk tolerance.	Risk Management Strategy
P-3: Risk Assessment - Organization	Assess organization-wide security and privacy risk and update the risk-assessment results on an ongoing basis.	Risk Assessments
P-4: Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional)	Establish, document, and publish organizationally tailored control baselines and/or Cybersecurity Framework Profiles.	No related finding during this audit.
P-5: Common Control Identification	Identify, document, and publish organization-wide common controls available for inheritance by organizational systems.	No related finding during this audit.

[1] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. ii (December 2018).

[2] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 28 (December 2018).

Risk Management Task Number	Task Description	Related Finding
P-6: Impact-Level Prioritization (Optional)	Prioritize organizational systems with the same impact level.	No related finding during this audit.
P-7: Continuous Monitoring Strategy - Organization	Develop and implement an organization-wide strategy for continuously monitoring control effectiveness.	Continuous Monitoring Strategy
P-8: Mission or Business Focus	Identify the missions, business functions, and mission/business processes the system is intended to support.	Documentation
P-9: System Stakeholders	Identify stakeholders who have an interest in the system’s design, development, implementation, assessment, operation, maintenance, or disposal.	Documentation Agency Process
P-10: Asset Identification	Identify assets that require protection.	Documentation Agency Process
P-11: Authorization Boundary	Determine the authorization boundary of the system.	Documentation
P-12: Information Types	Identify the types of information to be processed, stored, and transmitted by the system.	Documentation
P-13: Information Life Cycle	Identify and understand all stages of the information life cycle for each information type the process processed, stored, or transmitted.	Documentation
P-14: Risk Assessment - System	Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	Risk Assessments
P-15: Requirements Definition	Define the security and privacy requirements for the system and the environment of operation.	Privacy Requirements
P-16: Enterprise Architecture	Determine the system’s placement within the enterprise architecture.	No related finding during this audit.

Risk Management Task Number	Task Description	Related Finding
P-17: Requirements Allocation	Allocate security and privacy requirements to the system and the environment of operation.	Agency Process
P-18: System Registration	Register the system with organizational program or management offices.	No related finding during this audit.

Step 2: Categorize

The Categorize step informs organizational risk-management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information those systems processed, stored, and transmitted.[3]

Table B–2: Categorize Task

Risk Management Task Number	Task Description	Related Finding
C-1: System Description	Document the system's characteristics.	Documentation
C-2: Security Categorization	Categorize the system and document the security categorization results.	Documentation
C-3: Security Categorization Review and Approval	Review and approve the security categorization results and decision.	Documentation Agency Process

[3] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 46 (December 2018).

Step 3: Select

The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the nation.[4]

Table B–3: Select Tasks

Risk Management Task #	Task Description	Related Finding
S-1: Control Selection	Select the controls for the system and the environment of operation.	Security and Privacy Controls Privacy Requirements
S-2: Control Tailoring	Tailor the controls selected for the system and the environment of operation.	Documentation Agency Policies/Procedures
S-3: Control Allocation	Allocate security and privacy controls to the system and to the environment of operation.	Documentation Agency Policies/Procedures
S-4: Documentation of Planned Control Implementations	Document the controls for the system and environment of operation in security and privacy plans.	Documentation Agency Policies/Procedures Privacy Requirements
S-5: Continuous Monitoring Strategy – System	Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.	Agency Policy
S-6: Plan Review and Approval	Review and approve the security and privacy plans for the system and the environment of operation.	Documentation Agency Process Privacy Requirements

[4] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 50 (December 2018).

Step 4: Implement

The Implement step implements the controls in the security and privacy plans for the system and the organization and documents in a baseline configuration, the specific details of the control implementation.[5]

Table B–4: Implement Tasks

Risk Management Task Number	Task Description	Related Finding
I-1: Control Implementation	Implement the controls in the security and privacy plans.	Documentation Privacy Requirements Agency Policies/Procedures
I-2: Update Control Implementation Information	Document changes to planned control implementations based on the "as-implemented" state of controls.	Documentation Privacy Requirements Agency Policies/Procedures

Step 5: Assess

The Assess step determines whether the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.[6]

Table B–5: Assess Tasks

Risk Management Task Number	Task Description	Related Finding
A-1: Assessor Selection	Select the appropriate assessor or assessment team for the type of control assessment to be conducted.	Documentation
A-2: Assessment Plan	Develop, review, and approve plans to assess implemented controls.	Documentation Privacy Requirements Agency Process
A-3: Control Assessments	Assess the controls in accordance with the assessment procedures described in assessment plans.	Documentation Privacy Requirements

[5] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 58 (December 2018).

[6] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 61 (December 2018).

Risk Management Task Number	Task Description	Related Finding
A-4: Assessment Reports	Prepare the assessment reports documenting the findings and recommendations from the control assessments.	Documentation Privacy Requirements Agency Process
A-5: Remediation Actions	Conduct initial remediation actions on the controls and reassess remediated controls.	Documentation
A-6: Plan of Action and Milestones	Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports.	Documentation Agency Policies/Procedures

Step 6: Authorize

The Authorize step provides organizational accountability by requiring that a senior management official determine whether the security and privacy risk (including supply-chain risk) to organizational operations and assets, individuals, other organizations, or the nation based on the operation of a system or the use of common controls, is acceptable.[7]

Table B–6: Authorize Tasks

Risk Management Task Number	Task Description	Related Finding
R-1: Authorization Package	Assemble and submit the authorization package to the authorizing official for an authorization decision.	Privacy Requirements
R-2: Risk Analysis and Determination	Analyze and determine the risk from the operation or use of the system or the provision of common controls.	Agency Process
R-3: Risk Response	Identify and implement a preferred course of action in response to the risk determined.	Documentation

[7] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 69 (December 2018).

Risk Management Task Number	Task Description	Related Finding
R-4: Authorization Decision	Determine whether the risk from the operation or use of the information system or the provision or use of common controls is acceptable.	Documentation Agency Policies/Procedures
R-5: Authorization Reporting	Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.	Documentation Agency Policies/Procedures

Step 7: Monitor

The Monitor step maintains an ongoing situational awareness about the information system's security and privacy posture and the organization in support of risk management decisions.[8]

Table B–7: Monitor Tasks

Risk Management Task Number	Task Description	Related Finding
M-1: System and Environment Changes	Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.	Documentation Agency Policy
M-2: Ongoing Assessments	Assess the controls implemented within, and inherited by, the system in accordance with the continuous monitoring strategy.	Continuous Monitoring Strategy
M-3: Ongoing Risk Response	Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones.	Documentation Agency Policy

[8] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Rev 2*, p. 76 (December 2018).

Risk Management Task Number	Task Description	Related Finding
M-4: Authorization Package Updates	Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process.	Documentation Agency Policy
M-5: Security and Privacy Reporting	Report the system's security and privacy posture to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.	Agency Policy
M-6: Ongoing Authorization	Review the system's security and privacy posture on an ongoing basis to determine whether the risk remains acceptable.	Agency Process
M-7: System Disposal	Implement a system disposal strategy and execute required actions when a system is removed from operation.	No related finding during this audit.

Appendix C – AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: September 20, 2024 Refer To: TQA-1

To: Michelle L. H. Anderson
Acting Inspector General

From: Dustin Brown
Acting Chief of Staff

Subject: Office of the Inspector General Draft Report
(A-14-21-51093) – INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations.

Please let me know if I can be of further assistance. You may direct staff inquiries to Hank Amato at (407) 765-9774.

OFFICE OF THE INSPECTOR GENERAL ★ SOCIAL SECURITY ADMINISTRATION ★

OIG

Mission: The Social Security Office of the Inspector General (OIG) serves the public through independent oversight of SSA's programs and operations.

Report: Social Security-related scams and Social Security fraud, waste, abuse, and mismanagement, at oig.ssa.gov/report.

Connect: OIG.SSA.GOV

Visit our website to read about our audits, investigations, fraud alerts, news releases, whistleblower protection information, and more.

Follow us on social media via these external links:

X @TheSSAOIG

f OIGSSA

▶ TheSSAOIG

✉ Subscribe to email updates on our website.