Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Plans of Action and Milestones

142320 September 2025

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 30, 2025 **Refer to:** 142320

To: Frank Bisignano
Commissioner

From: Michelle L. Anderson
Acting Inspector General

Subject: Plans of Action and Milestones

The attached report summarized the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration managed its plan of action and milestones in accordance with Federal and Agency requirements.

Our full audit report contains information that, if not protected, could result in adverse effects to the Agency's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management our audit's detailed findings and recommendations and excluded from this summary certain sensitive information because of the potential damage if the information is misused. We determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices.

If you wish to discuss the final audit report or this audit summary, please call me or have your staff contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

Plans of Action and Milestones 142320

September 2025 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration (SSA) managed its plans of action and milestones (POAM) in accordance with Federal and Agency requirements.

Background

SSA uses POAMs to correct information security weaknesses identified by audits or vulnerability assessments done by, for, or on behalf of, the Agency. A POAM identifies the tasks required to address a security weakness. It also details the resources required, such as staff time or funding; sets milestones for completing tasks; and schedules completion dates for milestones.

The *Federal Information Security Modernization Act of 2014*, mandates that all Federal departments and agencies develop a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies.

POAMs play a crucial role in SSA's risk-management framework by documenting security weaknesses, remediation efforts, and timeframes. SSA uses POAMs as the primary method for tracking and addressing security risk.

Results

Although SSA had some policies, procedures, and practices to manage POAMs in compliance with Federal and agency requirements, SSA did not manage POAMs in compliance with Federal and Agency requirements.

Conclusion

Given the critical role of POAMs in safeguarding information systems, SSA must establish and manage them in accordance with Federal guidelines to ensure it takes appropriate and timely action to resolve security issues.

Recommendations

We made 13 recommendations, and SSA agreed to implement all of them.

TABLE OF CONTENTS

ABBREVIATIONS

NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POAM	Plan of Action and Milestone
Pub. L. No.	Public Law Number
SAM	Security Authorization Manager
SSA	Social Security Administration

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) managed its plans of action and milestones (POAM) in accordance with Federal and Agency requirements.

BACKGROUND

SSA uses POAMs to correct information security weaknesses identified by audits or vulnerability assessments done by, for, or on behalf of, the Agency. A POAM identifies the tasks required to address a security weakness. It also details the resources required, such as staff time or funding; sets milestones for completing tasks; and schedules completion dates for milestones.

The *Federal Information Security Modernization Act of 2014* mandates that all Federal departments and agencies develop a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies.[1] POAMs allow agency officials and oversight authorities to track whether agencies complete corrective actions timely.

According to the National Institute of Standards and Technology (NIST), Federal agencies should "[develop a POAM] for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies" and "[update] existing [POAM]s . . . based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities."[2] Furthermore, Federal agencies should review POAMs for consistency with their organizational risk-management strategy and priorities for risk-response actions.[3] POAMs play a crucial role in SSA's risk-management framework by documenting security weaknesses, remediation efforts, and timeframes. SSA uses POAMs as the primary method for tracking and addressing security risk.

SCOPE AND METHODOLOGY

We reviewed Federal requirements and SSA policies and procedures for establishing, managing, and closing POAMs. We also interviewed SSA personnel responsible for POAMs. We also reviewed random samples of Security Assessment Reports, 30 open POAMs, and 30 closed POAMs.

We determined whether each sampled met Federal and Agency requirements. See Appendix A for additional information about our scope and methodology.

---

[1] *Federal Information Security Management Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3080 (2014).

[2] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53*, *Revision 5*, sec. CA-5, p. 88 (December 2020).

[3] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53*, *Revision 5*, sec. PM-4.b, p. 205 (December 2020).

RESULTS OF REVIEW

Although SSA had some policies, procedures, and practices to manage POAMs, SSA did not do so in compliance with Federal and Agency requirements.[4]

Documenting Resources

According to Office of Management and Budget (OMB) guidance, a POAM must detail resources required to accomplish the elements of the remediation plan and must specify whether funds will come from a reallocation of base resources or a request for new funding.[5] Resources include personnel, new hard- or software, and tools required to complete the tasks necessary to address the identified deficiency. NIST notes that POAMs include ". . . tasks to be accomplished with a recommendation for completion before or after system authorization; resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks."[6]

SSA requires that the security authorization manager (SAM) enter a high-level summary of the actions needed to remediate the POAM and the milestones for addressing them, along with completion dates, into the security assessment tool. However, SSA does not require that the SAM enter the resources for the POAM. Although the tool includes a funding tab; SAMs are not required to complete it. Documenting resources could help the Agency identify, assess, prioritize, and monitor the progress of corrective efforts for identified weaknesses. Without documenting the required resources, SSA cannot determine the relative cost of POAMs, conduct cost-benefit analysis, or calculate the net value added by completing POAMs.

Following Procedures When Creating Plans of Action and Milestones

According to the National Institute of Standards and Technology (NIST), Federal agencies should "[d]evelop a [POAM] for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies".[7] We reviewed SSA's POAM creation process and found deficiencies.

---

[4] Our report contains information that, if not protected, could result in adverse effects to SSA's information systems. In accordance with government auditing standards, we have separately transmitted to SSA management our audit report, which details our findings and recommendations. We excluded from this summary certain sensitive information because of the potential damage if the information is misused. We have determined the omitted information neither distorts the audit results described in this report nor conceals improper or illegal practices. GAO, *Government Auditing Standards*, *GAO-18-568G*, pars. 9.61 through 9.67, pp. 208 through 210 (July 2018).

[5] OMB, *Guidance for Preparing and Submitting Security Plans of Action and Milestones, M-02-01*, p. 2 (2001).

[6] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *800-37 Revision 2*, p. 68 (December 2018).

[7] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53*, *Revision 5*, sec. CA-5, p. 88 (December 2020).

Reviewing and Updating Open Plans of Action and Milestones Quarterly

According to NIST, Federal agencies should "[update existing POAM]s . . . based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities."[8] We reviewed SSA's POAM update process and found deficiencies.

Closing Plans of Action and Milestones

When vulnerabilities are not remediated timely, the Agency's security posture is compromised, which could expose its sensitive data and information to unnecessary risk. Failing to meet required remediation timelines lengthens the period of exposure of Agency information, which may provide expanded opportunities for threat actors to access and exploit data. Timely and effective remediation of security weaknesses is essential to achieving a mature information security program. We reviewed closed POAMs and found deficiencies.

CONCLUSION

Given the critical role POAMs have in safeguarding information systems, SSA must establish and manage them in accordance with Federal guidelines to ensure it takes appropriate and timely action to resolve security issues. SSA needs to improve its POAM process to address known vulnerabilities and reduce exposure to such risks as cyber-attacks and data breaches. Delays and deficiencies in remediating security weaknesses significantly increases SSA's exposure to cyber-risks, including unauthorized access and compromised data integrity. Prompt and thorough remediation and validation are essential to protect operations and maintain secure, reliable systems.

RECOMMENDATIONS

We made 13 recommendations.

AGENCY COMMENTS

SSA agreed to implement our recommendations. See Appendix B for the full text of SSA's response.

[8] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53*, *Revision 5*, sec. CA-5, p. 88 (December 2020).

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal regulations and guidance related to managing and maintaining plans of action and milestones (POAM), including the following.
    - Office of Management and Budget Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (October 17, 2001);
    - National Institute of Standards and Technology *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *Special Publication 800-37*, *Revision 2* (December 2018); and
    - National Institute of Standards and Technology *Security and Privacy Controls for Information Systems and Organizations*, *Special Publication 800-53, Revision 5* (December 2020).
- Reviewed the Social Security Administration's (SSA) policies, procedures, and documentation pertaining to firewall administration.
- Selected a non-statistical sample of
    - 25 systems with an Authority to Operate as of December 1, 2024.
    - 30 POAMs closed between January 1, 2024 and December 1, 2024.
    - 30 POAMs open as of December 1, 2024.
- Reviewed supporting documentation, including
    - Security Assessment Reports;
    - POAM status reports; and
    - Evidence used for POAM closure.
- Interviewed SSA personnel responsible for managing and maintaining POAMs.

We conducted our audit from December 2024 through July 2025. The principal entity reviewed was the Office of Information Security within the Office of the Chief Information Officer. We assessed the reliability of the data obtained by ensuring it met the criteria of our request, included all data elements requested, and did not contain duplicates. Although we identified deficiencies with the POAM process, we determined that the data were sufficiently reliable for the purposes of our review.

We assessed the significance of internal controls necessary to satisfy the audit objective. This included an assessment of the five internal control components: 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 risks
- Component 3: Control Activities
  - Principle 10 – Design control activities
- Component 4: Information and Communication
  - Principle 13: Use quality information
  - Principle 14: Communicate internally
  - Principle 15: Communicate externally
- 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B AGENCY COMMENTS

SOCIAL SECURITY
Office of the Commissioner

MEMORANDUM

Date: September 26, 2025 Refer To: TQA-1

To: Michelle L. Anderson
Acting Inspector General

From: Chad Poist
Chief of Staff

Subject: Office of the Inspector General Draft Summary Report, "Plans of Action and Milestones" (142320) -- INFORMATION

Thank you for the opportunity to review the summary report. We have no comments.

Please let me know if I can be of further assistance. You may direct staff inquiries to Amy Gao at (410) 966-1711.

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

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:

@TheSSAOIG

OIGSSA

TheSSAOIG

Subscribe to email updates on our website.