



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 30, 2026

Refer To: 142302

To: Frank Bisignano
Commissioner

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

Subject: Insider Threat Program

The attached report summarizes the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration's Insider Threat Program complied 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 report, please call me or have your staff contact Jeffrey Brown, Deputy Assistant Inspector General for Audit.

Attachment

AUDIT REPORT

Objective

Our objective was to determine whether the Social Security Administration's (SSA) Insider Threat Program complied with Federal and Agency requirements.

Background

An insider is an employee or contractor who has authorized access to Agency resources, such as facilities, equipment, information, systems, and computer networks.¹ Insider threat is the risk an insider will, wittingly or unwittingly, use their authorized access to harm national security through espionage, terrorism, or the loss or degradation of Agency resources or capabilities.² Insider threat programs are intended to deter employees and contractors who could be insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative, or other response actions.

Executive Order 13587 requires that Federal agencies create an insider threat program and implement guidelines and standards issued by the Office of the Director of National Intelligence's National Insider Threat Task Force (NITTF).³ In November 2012, the NITTF issued its *National Insider Threat Policy*. The *Policy* focuses on strengthening and safeguarding Federal agencies to counter insiders who may use their authorized access to compromise sensitive information.⁴ The *Policy* established minimum standards for Executive Branch agencies' insider threat programs. The standards include

- developing a comprehensive agency insider threat policy;
- developing guidelines and procedures for documenting each insider threat matter reported and the response actions taken;
- providing all cleared employees insider threat awareness training; and
- verifying that all cleared employees have completed the required training.⁵

¹ NITTF, *National Insider Threat Policy*, p. 4 (November 21, 2012).

² NITTF, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, p. 5 (November 21, 2012).

³ *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Executive Order No. 13,587, 3 C.F.R. 13587, pp. 276 through 280 (October 13, 2011).

⁴ NITTF, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (November 21, 2012).

⁵ A cleared employee has been granted access to classified information; is employed by a department or agency, including a commercial contractor and all subcontractors; is a personal services contractor; or is any other category of person who acts for, or on behalf of, a department or agency as determined by the appropriate department or agency head. NITTF, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, p. 5 (November 21, 2012).

SSA generates, collects, and maintains personal and sensitive information for nearly every U.S. citizen, and the Agency's employees and contractors have access to SSA systems that they could leverage for illegal or harmful purposes. Consequently, an effective insider threat program is vital to protecting information in SSA's network and systems and should include controls to monitor, detect, and prevent insider threats.

According to SSA, in September 2025, the Commissioner of Social Security established a Security and Resiliency component to consolidate all security functions, including insider threat, into a single, integrated group responsible for executing and managing security functions throughout the Agency. In January 2026, SSA named a new Head of Insider Threat and Resiliency who also serves as SSA's Information Sharing and Safeguarding Senior Official in accordance with Executive Order 13587 and NITTF guidelines and standards. SSA believes this reorganization strengthens its ability to manage risk across the full employee lifecycle, from recruitment to separation.

Scope and Methodology

We reviewed SSA's policies and procedures as well as Federal guidance and regulations related to the insider threat program and met with SSA subject-matter experts to walk through the Agency's insider threat training program. We reviewed SSA's insider threat program management, training, personnel separation procedures, and data collection and analysis. For more information about our scope and methodology, see Appendix A.

Results of Review

SSA's Insider Threat Program did not fully comply with Federal and Agency requirements.⁶

Insider Threat Program Policy

Insider threats manifest in various ways including violence, espionage, sabotage, and theft and can include harm perpetrated in the cyber-domain. An insider threat program should mitigate the impact of these threats through appropriate management and enforcement actions. An effective insider threat program combines physical security, personnel assurance, and information-centric principles.⁷ The NITTF suggests agencies regularly review insider threat policies to ensure the guidance adapts to any changes to laws, policies, organizational structures, and/or information technology architecture.⁸ We reviewed SSA's *Insider Threat Program Policy* and found deficiencies.

⁶ Our 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 full 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).

⁷ Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide*, sec. 3, Building an Insider Threat Mitigation Program, p. 23 (November 2020).

⁸ NITTF, *2017 Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*, p. 17 (2017).

Insider Threat Training

A highly aware workforce is key to the early detection and prevention of malicious insider threat conduct. It is important to invest resources to continuously educate the workforce on the risks associated with insider threats. This includes training on how to recognize and report anomalies and indicators. Training drives home the message that vigilance is necessary because of the enormous damage that can be caused by malicious insiders.

Cleared Employees

Based on NITTF guidance, a “cleared employee” has access to classified information. This definition comprises individuals employed by a department or agency, including contractors and subcontractors, and any other category of person who acts for, or on behalf of, a department or agency, as determined by the appropriate department or agency head.⁹ Federal standards require that agencies provide insider threat awareness training to all cleared employees within 30 days of initial employment, entry on duty, or after granting access to classified information, and annually thereafter. Agencies must also verify that all cleared employees complete the required training.¹⁰ We reviewed SSA’s Insider Threat training program for cleared employees and found deficiencies.

Active Employees

Although Federal standards did not require that agencies provide insider threat awareness training to all employees, SSA’s policy exceeded minimum Federal expectations. We reviewed SSA’s Insider Threat training program for all employees and found deficiencies. While the Agency policy goes beyond the Federal requirement, it does not enforce the requirement with consequences for employees who do not complete the training. However, because the Agency’s training requirement exceeds Federal standards, we are not making a formal recommendation for corrective action.

Separated Personnel

Federal standards require that, upon an employee’s separation, agencies disable their systems access within an organization-defined time period and terminate or revoke any authenticators and credentials associated with the individual.¹¹ When the Agency cannot collect the employee’s personal identity verification card, normal termination procedures must be completed within 18 hours of their separation.¹² We reviewed a sample of separated personnel and found deficiencies.

⁹ NITTF, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, p. 5 (November 21, 2012).

¹⁰ NITTF, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, p. 4 (November 21, 2012).

¹¹ NIST, *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, Revision 5, sec. PS-4, pp.224 and 225 (updated December 10, 2020).

¹² NIST, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS 201-3, p. 26 (January 2022).

Insider Threat Reporting

Insider threat reporting is vital for safeguarding Federal agencies. Agency leaders must establish clear procedures to track and resolve cases, conduct regular self-assessments, and provide reports to regulatory bodies. A proactive approach that includes filing incident reports and annually updating insider threat policies helps protect sensitive information and critical assets and reinforces a culture of accountability and vigilance within the organization.

Incident Reports

Federal agencies are required to develop guidelines and procedures for documenting each insider threat matter reported and actions taken in response. Agencies must also ensure each matter is resolved timely.¹³ We reviewed a sample of SSA's documented insider threat inquiry reports and found deficiencies.

Annual Update to the National Insider Threat Task Force

Executive Order and SSA's own policy require that SSA conduct self-assessments of its compliance with insider threat policies and report the results annually to the NITTF's Senior Information Sharing and Safeguarding Steering Committee.¹⁴ We reviewed SSA's compliance with annual reporting requirements and found deficiencies.

Conclusion

SSA's responsibility for safeguarding sensitive information underscores the critical need for a robust insider threat program. Given the substantial risks posed by personnel with legitimate access to SSA systems, it is essential to implement comprehensive controls to monitor, detect, and prevent insider threats of all types. By implementing our recommendations, SSA could improve its insider threat program to ensure the ongoing integrity, security, and functionality of its network, systems, and operations.

Recommendations

We made six recommendations to SSA to improve its Insider Threat Program.

Agency Comments

SSA agreed to implement our recommendations; see Appendix B.

¹³ NITTF, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, p. 2 (November 21, 2012).

¹⁴ Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Executive Order No. 13,587, 3 C.F.R. 13587, pp. 276 through 280 (October 13, 2011).

APPENDIX A – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal regulations and guidance related to Insider Threat Programs.
 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Executive Order 13587 (October 7, 2001).
 - National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (December 2020).
 - National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS PUB 201-3, (January 2022).
 - National Insider Threat Task Force, *Insider Threat Program Maturity Framework* (October 24, 2018).
 - National Insider Threat Task Force, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (November 21, 2012).
- Reviewed best practices pertaining to insider threat programs.
 - Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide* (November 2020).
 - National Insider Threat Task Force, *2017 Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards* (2017).
- Reviewed the Social Security Administration's (SSA) policies, procedures, and documentation pertaining to its insider threat program.
- Reviewed training records for SSA employees.
- Selected non-statistical samples of and reviewed documentation for
 - insider threat inquiries and
 - personnel separated between July 1, 2024 and June 30, 2025.
- Interviewed SSA personnel responsible for managing and maintaining Insider Threat Program.

We assessed the reliability of the data provided 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 Insider Threat Program, we determined 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 1: Control Environment
 - Principle 5: Enforce accountability
- Component 2: Risk Assessment
 - Principle 6: Define objectives and risk tolerances
 - Principle 7: Identify, analyze, and respond to risks
 - Principle 8: Assess fraud risk
- Component 3: Control Activities
 - Principle 10: Design control activities
 - Principle 12: Implement 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
 - Principle 17: Evaluate issues and remediate deficiencies

We conducted our review between July 2025 and August 2026. The principal entity reviewed was the Office of Insider Threat and Resiliency within the Office of Security and Resiliency. 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 – AGENCY COMMENTS



MEMORANDUM

Date: September 25, 2026

Refer To: TQA-1

To: Michelle L. Anderson
Assistant Inspector General for Audit as First Assistant



From: Chad Poist
Chief Risk Officer

Subject: Office of the Inspector General Draft Memorandum "Insider Threat Program" (142302L) --
INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations. At Social Security, we are proud to administer benefit programs that millions of Americans have contributed to and rely on. We take our responsibility as stewards of these programs and trust funds seriously. While administering benefits, it is also our duty to securely maintain the public's data. We will continue to safeguard Social Security resources, ensuring benefits are issued only to those who qualify, while actively fighting fraud, waste, and abuse.

Please let me know if I can be of further assistance. You may direct staff inquiries to Amy Gao, Director of the Audit Liaison Staff.

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001