Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Role-based Training

142317 August 2025

Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: August 12, 2025 **Refer to:** 142317

To: Frank Bisignano
Commissioner

From: Michelle L. Anderson
Acting Inspector General

Subject: Role-based Training

The attached final report presents the results of the Office of Audit's review. The objective was to determine whether the Social Security Administration's role-based training complied with Federal and Agency requirements.

Please provide within 60 days a corrective action plan that addresses each recommendation. 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

Role-based Training
142317

August 2025 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) role-based training complied with Federal and Agency requirements.

Background

Each of SSA's over 50,000 employees and contractors plays a role in safeguarding the sensitive information individuals entrust to the Agency. For some, that role carries significant security and privacy responsibilities. Agency staff must understand their roles and effectively carry out security and privacy duties to protect personally identifiable information; reduce breaches or unauthorized disclosures of Agency information; and protect Agency information systems, data, and personnel from malicious attacks.

The Office of Management and Budget requires that Federal agencies provide role-based security and privacy training to employees and contractors before it authorizes them to access Federal information or information systems or perform assigned duties. Additionally, the National Institute of Standards and Technology requires that agencies provide role-based security and privacy training to personnel with organization-defined roles and responsibilities.

SSA requires that all information systems users with significant security and/or privacy responsibilities complete role-based security and privacy training each fiscal year.

Results

SSA's role-based security and privacy training program did not fully comply with Federal and Agency requirements, and we identified areas that increase security risk because SSA was not fully compliant. SSA did not

- assign role-based security training to executives who assumed their roles after SSA assigned training;
- ensure contractors completed required role-based security training; nor
- initially assign role-based privacy training to all required employees.

Recommendations

We recommend SSA:

1. Include terms or conditions in all contracts that require that contractors identified as having significant security responsibilities complete role-based security training before they perform their assigned duties and, at least, each fiscal year thereafter.
2. Implement data validation controls before it processes the role-based privacy training assignments to prevent errors and avoid confusion between different components.
3. Develop and implement a process to send stakeholders routine reminders to update personnel information and periodically validate that all stakeholder information is accurate.

SSA agreed to implement our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPD	Office of Privacy and Disclosure
OSLWD	Office of Strategy, Learning, and Workforce Development
SSA	Social Security Administration

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) role-based training complied with Federal and Agency requirements.

BACKGROUND

Each of SSA's over 50,000 employees and contractors plays a role in safeguarding the sensitive information individuals entrust to the Agency. For some, that role carries significant security and privacy responsibilities. Agency staff must understand their roles and effectively carry out security and privacy duties to protect personally identifiable information; reduce breaches or unauthorized disclosures of Agency information; and protect the Agency's information systems, data, and personnel from malicious attacks.

SSA's role-based training ensures personnel with significant security and privacy responsibilities maintain the skill sets to perform their critical functions.[1] Assigning role-based training is a multi-step process. Management must first define the significant work roles based on organization-defined roles and responsibilities and then identify the staff who are aligned with the designated work roles.[2]

The Office of Management and Budget (OMB) requires that Federal agencies provide employees and contractors role-based security and privacy training authorizing them to access Federal information and information systems or perform assigned duties.[3] Additionally, the National Institute of Standards and Technology (NIST) requires that agencies provide role-based security and privacy training to personnel with organization-defined roles and responsibilities and continue this training at agency-defined intervals.[4] Agencies should tailor training content to individuals' assigned roles and responsibilities in addition to the agency's security and privacy requirements and the systems to which personnel have authorized access.[5]

SSA requires that all information system users with significant security and/or privacy responsibilities complete annual role-based security and privacy training. This training is required in addition to the annual security awareness and privacy training provided to all employees and contractors.

---

[1] Role-based training includes specialized training on policies, procedures, and tools for individuals who are assigned roles having significant security and privacy responsibilities.

[2] NIST, *Building a Cybersecurity and Privacy Learning Program, 800-50, Revision 1,* sec. 2.5.4, p. 29 (September 2024).

[3] OMB, *Managing Information as a Strategic Resource*, Circular A-130, Appendix I, sec. 4.h.5, p. I-11 (July 28, 2016).

[4] NIST, *Security and Privacy Controls for Information Systems and Organizations*, *800-53, Revision 5*, sec. AT-3, p. 62 (December 2020).

[5] Refer to Footnote 4.

SCOPE AND METHODOLOGY

We reviewed Federal requirements and SSA policies and procedures related to role-based security and privacy training in September 2024.[6] We interviewed Agency personnel responsible for role-based security and privacy training and randomly sampled (1) 45 personnel with significant security responsibilities; (2) 45 personnel with significant privacy responsibilities; and (3) 45 information technology specific contracts. We reviewed each sampled item to determine whether it met Federal and Agency requirements. See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

The Agency's role-based security and privacy training program did not fully comply with Federal and Agency requirements. SSA partially complied with requirements by

- creating security and privacy training policies and procedures that comply with Federal and Agency requirements;
- establishing a systematic method to identify Agency personnel who require role-based security and privacy training;
- retaining evidence in the system of record that employees completed role-based security and privacy training;
- implementing controls to limit internet access when personnel did not complete role-based security training; and
- including sufficient material to cover all required role-based security and privacy training information.

We also identified areas with an increased security risk because SSA was not fully compliant. Specifically, SSA did not

- assign role-based security training to executives who assumed their roles after SSA assigned training;
- ensure contractors completed required role-based security training; or
- initially assign role-based privacy training to all required employees.

[6] SSA released updated role-based security training curriculum in January 2025; however, we did not review the new curriculum.

Security Training

SSA requires that personnel who have significant security responsibilities complete role-based security training each fiscal year. Employees are identified as having significant security responsibilities when they occupy a position assigned a National Initiative for Cybersecurity Education Framework role cyber-security code.[7] SSA's Office of Information Security uses an active employee roster from the Agency's Office of Human Resources, along with the identified position descriptions, to determine which employees the Office of Strategy, Learning, and Workforce Development (OSLWD) will assign the training. OSLWD releases the training in the 2nd quarter of each fiscal year, based on the existing active employee roster, and all identified employees must complete the training before the end of the fiscal year. Contract employees are not included in the population of personnel with significant security responsibilities. Instead, the Agency relies on the vendors to ensure their contractors complete the required training.

Agency Personnel

Executives in positions that required role-based security training, including then-Chief Information Officer and then-Deputy Commissioner of Systems, were not assigned the required training. This occurred because these executives assumed their positions after OSLWD developed the list of employees requiring training. The Agency did not have controls and policies in place to ensure employees who enter their positions after OSLWD assigns role-based security training complete the necessary training. Additionally, SSA did not assign training throughout the year; therefore, personnel who assumed significant security roles after the training was assigned may not have received the required training.

Without proper role-based training, executives may have performed a role and duties for which they were not fully trained. For example, an SSA executive may have signed a risk acceptance without having completed all the required training related to that duty.[8] By not ensuring executives complete the required role-based training, SSA sets a poor "tone at the top" regarding the importance of adhering to Federal standards.

After our review, SSA provided documentation that confirmed it had established controls to ensure applicable employees and executives receive role-based security training before they perform their assigned security-related duties. Therefore, we are not making a recommendation related to this finding.

Contractors

To maintain skill sets necessary to fulfill security job functions, vendors that provide the Agency contract services must ensure contracted personnel complete role-based security training each year. Additionally, the contract vendor must maintain evidence its personnel has completed training and must provide that evidence upon SSA's request.

---

[7] NIST, *Workforce Framework for Cybersecurity (NICE Framework), 800-181, Revision 1* (November 2020). The *NICE Framework* is a nationally focused resource that established a taxonomy and common lexicon to describe cyber-security work, and workers, regardless of where, or for whom, the work is performed and published by NIST.

[8] A risk acceptance is a document in which SSA formally acknowledges it has identified and accepts the risks associated with a specific program area.

For 20 of the 45 contracts we sampled, the vendor did not provide evidence its personnel had completed role-based security training. Vendors did not provide this information because SSA's contract did not include terms or conditions that required that contractors complete this training. Additionally, component managers and contracting officer representatives did not confirm contractors completed role-based security training or retain documentation of the completed training.

The lack of role-based security training terms or conditions in contracts limits SSA's ability to enforce compliance with its role-based security training requirements for contractors. In addition, SSA cannot ensure contractors with significant security responsibilities complete the necessary training, which increases the risk of security or data breaches and loss of sensitive information.

Privacy Training

SSA requires that individuals who have significant privacy roles and responsibilities complete role-based privacy training each fiscal year. SSA identifies these individuals as those with critical privacy workloads—those who work closely with the Agency's Office of Privacy and Disclosure (OPD) and are involved in developing, procuring, and implementing Agency systems that include processing personally identifiable information. OPD manually compiles the list of personnel by merging multiple lists, and OSLWD assigns the training to the identified individuals.[9]

We reviewed a sample of 45 employees identified as being subject to annual privacy role-based training requirements. Of the 45 employees, 43 had completed the training. OSLWD did not initially assign the required training for the remaining two employees[10] because the manual list OPD provided it contained incorrectly formatted and blank entries.[11] SSA's manual process lacked validation controls to detect these formatting issues, which led to confusion and resulted in missed training assignments.

Untrained employees may not have the knowledge to understand their privacy responsibilities and perform their duties effectively. Additionally, failing to assign role-based privacy training to all required employees poses a risk to SSA's information security posture and regulatory compliance. This error increases the risk of privacy violations, data breaches, and loss of sensitive information, such as personally identifiable information.

[9] SSA did not identify contractors as needing privacy role-based training. In October 2024, SSA instructed staff to include language in contracts that requires contractors to complete role-based privacy training, as required by SSA policy.

[10] During our audit, one individual was assigned and completed the training. OPD determined the second individual was not required to take the training.

[11] Some fields included multiple names, which led to individuals being overlooked when the training was assigned.

CONCLUSION

The Agency's role-based security and privacy training program does not fully comply with Federal and Agency requirements. The failure to assign role-based security and privacy training to all required personnel poses significant risk to SSA's information security posture and regulatory compliance. The lack of proper training increases the risk of privacy violations and the loss of sensitive information, including personally identifiable information. Furthermore, executives and other personnel who are unaware of their specific responsibilities related to security and privacy may inadvertently compromise Agency systems or fail to mitigate threats effectively.

RECOMMENDATIONS

We recommend SSA:

1. Include terms or conditions in all contracts that require that contractors identified as having significant security responsibilities complete role-based security training before they perform their assigned duties and, at least, each fiscal year thereafter.

2. Implement data validation controls before it processes the role-based privacy training assignments to prevent errors and avoid confusion between different components.

3. Develop and implement a process to send stakeholders routine reminders to update personnel information and periodically validate that all stakeholder information is accurate.

AGENCY COMMENTS

SSA agreed to implement our recommendations; see Appendix B.

APPENDICES

Appendix A — SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal laws, regulations, and guidance related to role-based training, including the following.
  - Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource* (July 2016);
  - National Institute of Standard and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53*, *Revision 5* (December 2020); and
  - NIST, *Building a Cybersecurity and Privacy Learning Program, Special Publication 800-50 Revision 1* (September 2024).
- Reviewed the Social Security Administration's (SSA) policies, procedures, and documentation pertaining to role-based training.
- Sampled 45 contracts to determine whether SSA's contract language required that contractors with significant security responsibilities complete role-based security training. Contracts were considered in scope if they were executed between January 1 and September 30, 2024, greater than $1 million, and information technology related.
- Sampled SSA personnel including contractors. We considered personnel who had significant security responsibilities or significant privacy responsibilities as of August 1, 2024.
  - Reviewed supporting documentation for 45 individuals who had significant *security* responsibilities to determine whether they completed the required role-based *security* training.
  - Reviewed supporting documentation for a sample of 45 individuals with significant *privacy* responsibilities to determine whether they completed the required role-based *privacy* training.
- Interviewed SSA personnel responsible for role-based security and privacy training.

We conducted our audit from August 2024 through April 2025. We assessed the reliability of the data by reviewing files for duplicate records and completed accuracy testing of the data. Although we identified deficiencies with the list of personnel with significant security and privacy responsibilities, we determined the data were sufficiently reliable for the purpose of the review. We provided a recommendation for SSA to address these findings.

The principal entities we reviewed were the Division of Security Customer Service under the Office of Information Systems within the Office of Chief Information Officer and the Office of Privacy and Disclosure under the Office of General Counsel within the Office of Law and Policy. 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 2: Exercise oversight responsibility
  - Principle 3: Establish structure, responsibility, and authority
  - Principle 5: Enforce accountability
- Component 3: Control Activities
  - Principle 10: Design control activities
  - Principle 12: Implement control activities
- Component 4: Information and Communication
  - Principle 14: Communicate internally
- 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 — AGENCY COMMENTS

SOCIAL SECURITY
Office of the Commissioner

MEMORANDUM

Date: July 28, 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 Report, "Role-based Training" (142317) -- INFORMATION

Thank you for the opportunity to review the draft report. We agree with the recommendations. We will encourage our stakeholders to utilize the Learning Management System as a valuable resource for their training assignments while ensuring compliance to all relevant federal mandates.

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

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.