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.