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.