Claims-taking Systems Access Profiles
A-14-17-50096

SOCIAL SECURITY ADMINISTRATION
OIG

February 2018 **Office of Audit Report Summary**

Objectives

To determine whether the Social Security Administration (SSA) (1) assigned its claims-taking (CT) profiles only to users who needed them to perform their duties and (2) properly limited the resources included in those profiles.

Background

In Fiscal Year 2017, SSA paid nearly $1 trillion in benefits. The Agency's claims-takers played a key role in administering these benefits by reviewing and authorizing claims. Of the Agency's nearly 60,000 employees, almost 20,000 rely on SSA's information technology systems to take claims for Social Security benefits.

The Agency requires that managers authorize employee access to SSA information systems based on need to know and limit access to the least privilege required to perform job functions. SSA uses system profiles to separate duties among its users.

Each profile contains permissions to access such system resources as software applications, data files, and transactions. Based on users' job duties, SSA assigns one or more profiles to their personal identification numbers. Users can then access the system resources included in their assigned profile(s).

Findings

SSA generally assigned its CT profiles only to users who needed them to perform their duties. However, we found SSA did not maintain a list of incompatible duties for claims-takers. In addition, SSA could further limit the (1) assignment of CT profiles to only those users who needed them to perform their duties and (2) resource permissions in its CT systems access profiles.

Recommendations

We recommend SSA:

1. Document incompatible CT duties and provide detailed guidance to ensure staff considers these conflicts when assigning or changing CT profiles.
2. Confirm the need for profile assignments of those who had not used a CT profile in longer than 1 year.
3. Review the list of non-CT positions for which CT profiles had been assigned and remove the assignments from users when they conflict with the principles of least privilege, need to know, and/or separation of duties.
4. Review the list of eight personal identification numbers that have at least five additional profiles to determine the appropriateness of the assignments.
5. Remove the 29 resource permissions in its CT profiles that have not been used in over 1,095 days.
6. Ensure the Agency's automated resource permission removal tool is operating properly.
7. Determine whether it would be appropriate to remove resource permissions before 1,095 days of nonuse.
8. Explore the feasibility of implementing a control that identifies non-use of resource types excluded from the Agency's automated resource permission removal tool and removes the resource permissions whose non-use exceeds management's threshold.

The Agency agreed with our recommendations.