Summary of Access to Social Security Administration Data at the Disability Determination Services
A-15-11-01127

January 2013

Objective

To determine whether (1) security profiles assigned to disability determination services (DDS) employees provide access to Social Security Administration (SSA) data they do not need, (2) terminated DDS employees continue to have access to SSA systems, and (3) DDSs have an appropriate process for requesting and approving access to SSA systems.

Background

SSA's systems access policy is built on the principles of least privilege and need-to-know. Controlling and limiting systems access to the Agency's information systems and resources is the first line of defense in assuring the confidentiality, integrity, and availability of the Agency's information technology resources.

Our Findings

DDSs have a responsibility to safeguard sensitive SSA data entrusted to them to ensure SSA DDS systems are not compromised. We reviewed DDS employees' systems access at 14 DDSs nationwide. Although the Agency has controls in place to review DDS employee access, we found that DDS employees were granted unnecessary access. We noted that DDS employees were assigned profiles that were not appropriate for their job functions and profiles that had not been used for an extended period of time. We also found that there was not a consistent process among the DDSs for removing access of terminated employees. This potentially led to the untimely removal of access for several employees. By not removing separated employees' system access timely, personnel may have inappropriate access to SSA systems. DDSs should formally document the processes for obtaining and removing access to ensure procedures are followed consistently. We found that several DDSs did not have formally documented policies and procedures.

Our Recommendations

Because the issues noted above have previously been identified as part of the Fiscal Year 2011 Financial Statement Audit and are still ongoing, we recommend that the Agency strengthen various policies to ensure that systems access for DDS employees is monitored and maintained properly.

The Agency agreed with our recommendations.