Report Summary

Social Security Administration Office of the Inspector General

July 2011

Objective

To determine whether the Social Security Administration's (SSA) managing and monitoring of nonfinancially significant local profiles compromised the security of its information; information systems; personnel; or other resources, operations, or assets.

Background

SSA has two types of profile ownership: corporate and local. Unlike corporate profiles, security staff can create local profiles without putting the profiles through a formal, multi-component approval process.

In Fiscal Year 2009, we found weaknesses in SSA's use of financially significant local profiles. Since our testing of Fiscal Year 2009 nonfinancially significant local profiles was limited, we initiated this review.

To view the full report, visit http://www.ssa.gov/oig/ADOBEPDF/A-14-10-20106.pdf

The Social Security Administration's Managing and Monitoring of Local Profiles

(A-14-10-20106)

Our Findings

Nothing came to our attention that compromised the security of the Agency's information; information systems; personnel; or other resources, operations, or assets. Although the population of local profiles decreased from 2009 to 2010, any mismanagement of these profiles could present an opportunity for those who know access control vulnerabilities to compromise SSA data. We believe the possibility of a compromise will diminish if SSA implements its plans to decrease the number, and restrict the use, of local profiles.

We found periods of nonuse greater than 1 year for profiles, datasets, and users. Employees who have not used their profiles or accessed datasets for at least 1 year should have their access needs reviewed.

Our review of SSA's secondary UserID policies and procedures identified conflicting scopes and undefined terminology that may have contributed to inconsistent compliance with secondary UserID policy.

Our Recommendations

SSA should:

1. Continue with its plans to reduce the number, and restrict the use, of local profiles.

2. Periodically review the Information Technology Resource Usage Report to identify individuals whose periods of non-access would warrant further review for continued access. Once reviewed, modify or revoke access, if needed, to comply with the access control principles of least privilege and need to know.

3. Develop a secondary UserID control policy that is clear, concise, and consistent.

SSA agreed with our recommendations.