Report Summary

Social Security Administration Office of the Inspector General

October 2011

Objective

To determine whether the Social Security Administration's current and proposed (SSA) electronic Authentication (eAuthentication) process creates a strong, secure authentication protocol that meets Federal guidelines and standards.

Background

SSA is expanding its Internet services to guide the public toward performing more business electronically. Some Internet applications involve the exchange of personally identifiable information. While these services may be more useful, they carry a greater risk of inappropriate disclosure.

In December 2003, the Office of Management and Budget issued guidance to ensure online Government services are secure and privacy is protected. The guidance requires that agencies review electronic transactions to ensure that authentication processes implemented provide appropriate assurance.

To view the full report, visit http://oig.ssa.gov/audits-and-investigations/audit-reports/A-14-11-11115

Report: The Social Security Administration's eAuthentication Process (A-14-11-11115)

Our Findings

SSA took steps to implement an eAuthentication process that included key elements needed to create a strong, secure authentication protocol for Level 2 citizen-to-government Internet applications and adopted an acceptable methodology for conducting risk assessments. The Agency is developing a National Institute of Standards and Technology compliant authentication protocol for Level 3 citizen-to-government Internet applications. However, we identified areas that needed improvements in the Agency's eAuthentication process to ensure compliance with Federal guidelines and standards.

- Four risk assessments were not documented.
- Documentation was insufficient to determine that risks were mapped to appropriate assurance levels for four applications.
- A National Institute for Standards and Technology-compliant security protocol for Level 3 citizen-to-government applications had not been implemented.
- Validations confirming applications achieved their assurance level were not performed after release to production.
- Periodic reassessments were not performed to reflect technology or business changes for 11 citizen-to-government

Our Recommendations

The Agency should: (1) perform required risk assessments for the four applications identified in this report; (2) map identified risks to applicable assurance levels for the four applications identified in this report; (3) reassess the three Level 3 applications; (4) continue development and implementation of the electronic Authentication system or an appropriate Level 3 authentication protocol; (5) establish a process that validates citizen-to-government Internet applications operationally achieved their required assurance level after release to production; and (6) conduct periodic reassessments when applicable, for citizen-to-government applications, to ensure identity authentication requirements continue to be valid in light of changes in technology or Agency business processes.

The Agency agreed with our recommendations.