Report Summary

Social Security Administration
Office of the Inspector General

Effective Use of Encryption Technology to Protect the Social Security Administration's Information Assets (Limited Distribution) (A-14-02-12048)

Our objective was to determine whether the Social Security Administration (SSA) is complying with established guidance for the use of encryption in protecting the transmission and storage of its sensitive information. SSA's distributed data processing environment requires it to store sensitive information and transmit it over telecommunications lines. Potentially, unauthorized individuals could intercept and monitor these transmissions, compromising the confidentiality of the information they contain if it is not adequately protected.

Encryption is the process of translating data into an encoded format, thereby rendering data unintelligible to unauthorized users and helping to protect the integrity of transmitted or stored data. SSA's evolving security structure and increasing emphasis on networked applications provide opportunities to improve the protection of its information assets through encryption. The Agency already uses encryption for this purpose in a number of applications.

Our review found that SSA could strengthen its information assets by having formalized encryption policy and procedures applied consistently throughout the Agency for applications housing sensitive information.

We recommended SSA centralize encryption monitoring and control functions within its evolving security structure to ensure consistent matching of encryption technology to risk throughout the Agency. The Agency disagreed with this recommendation, believing that its current structure and guidance is sufficient. We believe, however, that our recommendation will be fully addressed when the Agency issues its revised encryption policy. Our recommendation is consistent with the Agency's implemented organizational changes and planned policy changes.

We also recommended SSA develop a comprehensive policy which identifies the roles, functions, and responsibilities of individuals involved in the encryption process. This policy would also require that responsible staff members certify that the encryption process conforms to the provisions contained within the policy. SSA partially agreed with this recommendation. It is developing a more comprehensive encryption policy, but we continue to be concerned that it has not developed a plan to enforce the new policy and ensure it is consistently applied throughout the organization.

We further recommended SSA develop a risk-based approach or set of procedures to be applied to current and all new Agency information resources when matching the risks they present with appropriate encryption. Specifically, the approach would use common criteria to determine the level of sensitivity of the information processed or stored by applications,

portable devices, and other information resources. The sensitivity would be the basis used to apply an adequate level of cryptographic protection. SSA fully agreed with this recommendation.

This report contains information that is sensitive and confidential. For security reasons, distribution of this report was limited to those with a need to know.