FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Assessing Social Security Administration's Efforts to Protect Sensitive Information

September 2006 A-14-07-27068

Patrick P. O'Carroll, Jr. – Inspector General

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: September 22, 2006 Refer To:

To: The Commissioner

From: Inspector General

Subject: Assessing Social Security Administration's Efforts to Protect Sensitive Information (A-14-07-27068)

OBJECTIVE

Our objective was to assess the Social Security Administration's (SSA) actions to ensure that Personally Identifiable Information (PII) is safeguarded in accordance with the Office of Management and Budget (OMB) Memorandum M-06-16, *Protection of Sensitive Agency Information.*

BACKGROUND

In response to numerous incidents involving the compromise or loss of sensitive personal information, OMB issued several memoranda to provide Federal agencies guidance on the protection of PII entrusted to them.

OMB defined Sensitive PII as:

> …any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.[1]

Information systems can be either electronic or manual.

[1] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

OMB issued Memorandum M-06-16, on June 23, 2006. The Memorandum specifies measures that agencies need to have in place to ensure protection of sensitive remote information[2] by August 7, 2006.[3] M-06-16 requires Federal agencies to comply with the Security Checklist provided by National Institute of Standards and Technology (NIST) and recommends four additional actions that agencies should take for the protection of remote sensitive information. The intent is to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location.

The security controls and assessment procedures in the NIST Security Checklist were taken from NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005 and NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006. The controls and assessment methods/procedures in the checklist are a subset of what is currently required for moderate and high impact information systems.

SCOPE AND METHODOLOGY

Our work was limited to assessing SSA's efforts to protect sensitive information as prescribed by OMB Memorandum M-06-16. To meet our objective, we interviewed appropriate Agency staff and reviewed relevant Agency policies and procedures and controls' documentation. We used the review guide and the Data Collection Instrument developed by the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency. See Appendix B for more details on our Scope and Methodology.

SUMMARY OF RESULTS

Our assessment showed that SSA has taken a number of steps to comply with OMB Memorandum M-06-16 requirements. Based on our assessment, we found that the Agency has taken the following actions to protect its sensitive personal information;

- SSA has initiated projects to encrypt all laptop computers and mobile devices.
- On June 6, 2006, SSA's Chief Information Officer (CIO) issued a message to all SSA employees, contractors and Disability Determination Service employees to remind them of their responsibilities to properly safeguard PII entrusted to them.
- SSA has also created a web page *Safeguarding Personal Information,* where PII is defined and PII protection issues are discussed.
- SSA computers and applications are set to time out after 15 minutes of inactivity.

[2] Remote information is information that is either accessed remotely or physically transported outside of the agency's secured, physical location.

[3] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, page 1, June 23, 2006.

SSA continues to make progress in the protection of the PII. However, to fully comply with OMB Memorandum M-06-16 and to better protect remote PII, SSA needs to improve in the following areas:

- SSA policy for the protection of PII;
- Encryption of removable media;
- Encryption of sensitive data on mobile computers and devices;
- Two-factor authentication when remotely accessing PII; and
- Logging data extracts.

SSA Policy for the Protection of PII

SSA's information security policy is documented in its Information Systems Security Handbook (ISSH). During our review, we identified Agency policies and procedures regarding the protection of PII. For example, the memorandum issued by the CIO states "Mainframe access from the alternate duty station for those employees on flexiplace is prohibited." However, a number of important points in OMB Memorandum M-06-16 are not addressed. For example, SSA does not explicitly state whether downloading of PII is allowed. Also, the policy does not clearly state what remote access methods should be used. To comply better with OMB Memorandum M-06-16, SSA needs to revise and consolidate its security policy.

Encryption of Removable Media

OMB Memorandum M-06-16 recommends encryption for PII being transported and/or stored offsite.[4] SSA routinely sends its systems and data back-up tapes to off-site storage facilities (OSSF). There are about 20,000 tapes stored at its primary OSSF which contain PII. Currently, these tapes are not encrypted before they are sent for off-site storage. However, there are numerous compensating controls to protect these tapes such as storage in a secured vault, guards, and video monitoring. SSA is also in the process of evaluating an off-site data encryption solution to address this issue. In addition, SSA has implemented stringent physical security controls to protect these tapes during transportation to and within the storage facility.

Encryption of Sensitive Data on Mobile Computers and Devices

OMB Memorandum M-06-16 recommends encryption of all data on mobile computers and devices that carry sensitive agency data.[5] SSA has actively pursued the encryption of data on all mobile devices and has initiated a project to encrypt the hard drives of all laptop computers. All new laptops should have been encrypted by August 31, 2006 and all older laptops should be encrypted by October 31, 2006. In the future, SSA plans to decommission unencrypted laptops.

Additionally, SSA's Outlook Web Access (OWA) enables employees to access their SSA mailboxes from any computer which has Internet access. Employees can use their home

[4] OMB M-06-16, supra at page 1 and 6.

[5] Id.

computers to obtain full access to e-mail attached files through OWA. Although SSA requires password protection for such files, it does not ensure files containing PII are encrypted. SSA is working on a solution that will increase the security of data accessed through OWA. See section on two-factor authentication.

Two-Factor Authentication When Remotely Accessing PII

OMB Memorandum M-06-16 recommends that agencies allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.[6] SSA employees can access PII remotely through two methods, a virtual private network (VPN) and OWA. SSA's VPN can only be used on SSA computers configured to use SSA's VPN. The VPN technology uses two-factor authentication method: Smartcard (separate from the computer gaining access) and a password.

To access OWA, an individual uses his/her SSA network Personal Identification Number and password. However, the Office of Telecommunications and Systems Operations is developing and testing improved authentication methods to meet the requirements set forth by OMB Memorandum M-06-16.

Logging Data Extracts

OMB Memorandum M-06-16 recommends that agencies "log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required."[7] SSA acknowledged that it has not logged all of its data extracts nor verified that they were erased within 90 days.

SSA stated that this OMB recommendation poses a significant business concern and has serious implications for many existing SSA business processes. SSA routinely and extensively extracts data from its databases that contain PII and shares this information with both internal and external entities. Internally, SSA components use the data extracts within the organization for its core business processes and various reviews. Externally, SSA provides data extracts to other Federal, state and local government partners and trusted-third parties to assist in cross-agency program delivery and coordination.

Due to the large number of the data extracts created daily, SSA stated that it cannot log and track this information in accordance with OMB Memorandum M-06-16. However, the Agency has other compensating controls to protect the PII contained in the data extracts. They include access controls, certain logging activities, internal and external security audits, and the implementation of a new confidentiality notice transferring custodial responsibilities for protecting PII. SSA should continue to pursue its efforts to protect data extracts involving PII.

---

[6] OMB M-06-16, supra at page 1.

[7] Id.

CONCLUSIONS AND RECOMMENDATIONS

Our assessment showed that SSA has taken a number of steps to comply with OMB Memorandum M-06-16 requirements and has made progress in the protection of the PII. SSA has initiated projects to encrypt all laptop computers and mobile devices and has issued a reminder to its employees to remind them of their responsibilities to properly safeguard PII entrusted to them. SSA has also created a web page *Safeguarding Personal Information*, where PII is defined and PII protection issues are discussed. However, there are a few areas in the protection of remote PII that need to be addressed. To fully comply with OMB M-06-16, we recommend SSA:

1. Revise and consolidate Agency policy to better protect PII;

2. Continue to investigate methods to encrypt PII stored off-site and implement technologies that meet recommended NIST standards;

3. Complete on-going projects to encrypt all mobile computers and devices;

4. Implement stronger authentication solutions for OWA; and

5. Continue efforts to log and protect data extracts involving PII per NIST standards.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

DCI	Data Collection Instrument
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
ISSH	Information Systems Security Handbook
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OSSF	Off-site Storage Facility
OWA	Outlook Web Access
PII	Personally Identifiable Information
SP	Special Publication
SSA	Social Security Administration
VPN	Virtual Private Network

Scope and Methodology

The following is taken from the review guide developed by the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency.

Various laws and regulations have addressed the need to protect sensitive information held by government agencies including the Federal Information Security Management Act (FISMA), the E-Government Act of 2002, the Privacy Act of 1974, and the Office of Management and Budget's (OMB) Circular A-130, *Management of Federal Information Resources*. FISMA requires agencies to have a security program and controls for systems to protect their sensitive information. [1]

FISMA also requires agencies to implement standards and guidelines developed by the National Institute of Standards and Technology (NIST). [2] Relevant standards are:

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006; and
- FIPS Publication 201, *Personal Identity Verification of Federal Employees and Contractors*, February 2005.

Additional guidance on protecting PII and other sensitive information is described in NIST Special Publication (SP) 800 series. Among them, SP 800-53, *Recommended Security Controls for Federal Information Systems,* provides key criteria for assessing compliance with FISMA requirements. This guidance forms the basis for the OMB Memorandum M-06-16 Security Checklist covering protection of remote information. OMB's memorandum conveys the intent of implementing the checklist and specific recommended actions to be taken by Federal agencies for the protection of sensitive information to compensate for the lack of physical security controls when information is removed from, or accessed from outside the agency location. [3]

The following documents were considered with this review:

- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* September 2003;
- OMB Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 2003;

[1] Public Law 107-347, Title III, Section 301, 44 U.S.C. § 3541.

[2] Public Law 107-347, Title III, Section 302, 44 U.S.C. § 11331.

[3] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, page 1, June 23, 2006.

- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006;
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 2006;
- OMB Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006;
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006;
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005;
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006;
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels*, June 2004;
- Public Law 107-347, E-Government Act of 2002, Titles II and III;
- OMB Circular A-130, *Management of Federal Information Resources*, November 2000; and
- The Privacy Act of 1974; 5 U.S.C. 552a.

To meet our objectives, we interviewed appropriate Agency staff and reviewed relevant Agency policies and procedures and controls documentation. We completed our work in August and September 2006 in accordance with the review guide developed by the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Data Analysis and Technology Audit Division
(410) 965-9702

Phil Rogofsky, Audit Manager, Network Security and Telecommunications Branch
(410) 965-9719

Acknowledgments

In addition to the persons named above:

Grace Chi, Auditor-in-Charge

Mary Ellen Fleischman, Senior Program Analyst

Harold Hunter, Senior Auditor

Evelyn Chao, Auditor

Annette DeRito, Writer/Editor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-14-07-27068.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Executive Operations (OEO). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Executive Operations

OEO supports OIG by providing information resource management and systems security. OEO also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OEO is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.