FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2010
Evaluation of the Social Security Administration's Compliance with the *Federal Information Security Management Act*

A-14-10-20109

OFFICE OF THE INSPECTOR GENERAL

USA

SOCIAL SECURITY ADMINISTRATION

November 2010

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: November 10, 2010 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2010 Evaluation of the Social Security Administration's Compliance with the *Federal Information Security Management Act* (A-14-10-20109)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) overall security program and practices complied with the requirements of the *Federal Information Security Management Act of 2002* (FISMA) for Fiscal Year (FY) 2010.[1]

BACKGROUND

FISMA provides the framework for securing the Government's information and information systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of their security programs. FISMA requires that each agency develop, document, and implement an agency-wide information security program.[2]

OMB uses information reported pursuant to FISMA to evaluate agency-specific and Government-wide security performance, develop the annual security report to Congress, and assist in improving and maintaining adequate agency security performance. OMB issued Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* on April 21, 2010. OMB continues to require that agencies use a Web platform, CyberScope, to submit the annual FISMA report.

In the FY 2010 FISMA guidance, OMB stated that "[a]gencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way…. To do this, agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information. Agencies need to develop automated risk models and

[1] Pub. L. No. 107-347, Title III, Section 301.

[2] Pub. L. No. 107-347, Title III, Section 301 § 3544(b), 44 U.S.C. § 3544(b).

apply them to the vulnerabilities and threats identified by security management tools."[3] OMB also stated "[a]ny reporting should be a by-product of agencies' continuous monitoring programs and security management tools."[4] Agencies should provide direct feeds from their security management tools to CyberScope. For those agencies that do not have this ability, OMB will soon release a roadmap that will allow agencies to upload data from security management tools to CyberScope.[5]

This year, OMB instructed the Inspectors General (IG) to focus on their respective agency's management performance, in line with the requirements of FISMA.[6] The IGs were asked to assess agency performance in 10 major FISMA programs.[7] IGs were also required to determine areas for significant improvement if any agency programs did not have these key attributes.[8]

See Appendix B for OMB's 10 major FISMA programs and the required attributes for each program and Appendix C for additional background.

SCOPE AND METHODOLOGY

FISMA directs each agency's IG or an independent external auditor, as determined by the agency's IG, to perform an annual, independent evaluation of the effectiveness of the agency's information security program and practices.[9] SSA's Office of the Inspector General (OIG) contracted with Grant Thornton LLP (GT) to audit SSA's FY 2010 financial statements.[10] Because of the extensive internal control system review that is completed as part of that work, the OIG's FISMA requirements were incorporated into GT's financial statement information technology (IT) related work. This evaluation included the *Federal Information System Controls Audit Manual* (FISCAM) level reviews of SSA's financial-related information systems. GT also performed an "agreed-upon procedures" engagement using FISMA, OMB, National Institute of Standards and Technology (NIST) guidance, FISCAM, and other relevant security laws and regulations

[3] OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, page 1, April 21 2010.

[4] OMB M-10-15, supra at page 2.

[5] Id.

[6] OMB M-10-15, supra at page 3.

[7] Id.

[8] OMB M-10-15, supra, requires all reporting through CyberScope, page 2. The OMB-specified attributes for each program and the significant improvement examples are required to be posted on OMB's CyberScope Website, if necessary. The agency Chief Information Officers and IGs report through CyberScope.

[9] Pub. L. No. 107-347, Title III, Section 301, 44 U.S.C. § 3545(b)(1).

[10] OIG Contract Number GS-23F-8196H, December 3, 2009. FY 2010 option was exercised in December 2009.

as a framework to provide information and documentation for the required OIG review of SSA's information security program, practices, and information systems. See Appendix D for more details on our Scope and Methodology.

SUMMARY OF RESULTS

Based on the results of OIG and GT's work, we determined that SSA's security programs and practices generally complied with FISMA requirements for FY 2010; however, there were areas that needed improvement. SSA continues to work toward maintaining a secure environment for its information and systems. For example, SSA continues to have consistent processes in a number of areas including, certification and accreditation (C&A), vulnerability remediation, security training, remote access, continuous monitoring, and account and identity management.

Although the Agency continues to protect its information and systems, our FY 2009 audit identified, and GT's FY 2010 financial statement audit identified, certain deficiencies in internal controls that aggregated to a significant deficiency for financial statement reporting. It should be noted that a financial statement significant deficiency in internal control does not necessarily rise to the level of a significant deficiency as defined in FISMA.[11] The FY 2010 financial statement audit significant deficiency does not rise to the level of a significant deficiency under FISMA because of other compensating controls the Agency has in place, such as intrusion detection systems, guards, closed circuit televisions, automated systems checks, configuration management, and firewalls.

We also noted that SSA needed to improve certain aspects of security over its systems and sensitive information. SSA should ensure

- implementation of effective change control and access control processes;
- full implementation of an oversight program for systems operated by contractors or other entities on the Agency's behalf;

[11] The definition **of a significant deficiency for financial statement internal control** is provided by the Statement on Auditing Standards No. 115 (SAS 115) *Communicating Internal Control-Related Matters Identified in an Audit.* SAS 115 states a significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A **material weakness** is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. OMB provided the definition of **a significant deficiency under FISMA in its** *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* April 21, 2010, page 23 defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

- protection of personally identifiable information (PII);[12]
- proper incident handling and notification;
- continued improvement in its C&A process;
- continued improvement in its contingency planning;
- full implementation of its vulnerability remediation policy;
- employees and contractors receive security awareness and specialized security training; and
- continued implementation of a continuous monitoring program.

IMPLEMENTATION OF EFFECTIVE CHANGE CONTROL AND ACCESS CONTROL PROCESSES

OMB Circular A-123 Significant Deficiency

Controlling and limiting systems access to the Agency's information systems and resources is the first line of defense in ensuring the confidentiality, integrity, and availability of the Agency's information resources.[13] Lack of adequate access controls compromises the completeness, accuracy, and validity of the information in the system.

In FY 2009, our audit of SSA's financial statements identified a significant deficiency[14] in the Agency's control of access to its sensitive information.[15] In FY 2010, GT's audit of SSA's financial statements identified a significant deficiency in the Agency's change control management and access to sensitive information.[16]

In FY 2009, we reported that SSA needed to periodically recertify individuals' security accesses to Agency mainframe computers.[17] Moreover, a policy had not been established and consistently implemented Agency-wide to periodically reassess the content of security access to ensure employees and contractors are given least-privilege accesses for their job responsibilities. Further, SSA was unable to consistently

[12] OMB, M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* page 1, July 2006, defines 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 that 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 that is linked or linkable to an individual.

[13] SSA, Information Systems Security Handbook, Section 2.1.

[14] See Footnote 11.

[15] SSA OIG, *Fiscal Year 2009 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act* (A-14-09-19047), November 2009.

[16] Grant Thornton LLP, *Independent Auditor's Report* on SSA's FY 2010 Financial Statements, November 8, 2010.

[17] See Footnote 15.

provide evidence that Agency management reviewed security accesses or "profiles"[18] to determine whether system data, transactions, and resources for financially significant applications, systems, and related tools were in line with the concept of least privilege.

In FY 2010, GT identified the same issues we reported in FY 2009 and one new issue. Specifically, GT found that (1) SSA did not consistently comply with policies and procedures to reassess periodically the content of security access profiles; (2) some employees and contractors had system access that exceeded the access required to complete their job responsibilities; and (3) certain mainframe configurations increased the risk of unauthorized access.[19] Regarding the mainframe configuration issue that GT found this year, GT reported that some of SSA's employees and contractors were provided excessive access.[20] For example, an individual could have modified information or crashed the system. Once GT discovered the control weakness, SSA took immediate action to resolve it. GT recommended that SSA implement a policy that would require a periodic review of the content of the Agency's profiles and controls to test and monitor configurations on the mainframe.

According to the Office of the Chief Information Officer (OCIO), SSA has undertaken an IT project to address the access control weakness related to the significant deficiency. This project, once implemented, will provide enhanced capabilities for reviewing, approving and documenting the justifications associated with access requests.

FULL IMPLEMENTATION OF AN OVERSIGHT PROGRAM FOR SYSTEMS OPERATED ON THE AGENCY'S BEHALF BY A CONTRACTOR OR OTHER ENTITIES

FISMA requires that agencies protect information collected or maintained by, or on behalf of, agencies from unauthorized access, use, disclosure, disruption, modification or destruction.[21] Agencies' documented information security program should provide for information security for information and information systems provided or managed by another agency, contractor, or other source (Contractor System).[22] OMB's FISMA guidance states that agency information security programs apply to all organizations (sources) that possess or use Federal information – or that operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency. [23] Federal security requirements continue to apply, and the agency is

[18] A profile is one of TOP SECRET's primary access control mechanisms. Each profile contains a unique mix of facilities and transactions that determines what access to systems resources that specific position needs. TOP SECRET is a commercial access-control package modified to fit SSA's unique requirements and operating environment, provides security for SSA systems.

[19] SSA's FY 2010 Performance and Accountability Report.

[20] Additional details about this control weakness might further compromise SSA's information and information system, therefore, they are not provided in the report.

[21] Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A)(i), 44 U.S.C. § 3544(a)(1)(A)(i).

[22] Pub. L. No. 107-347, Title III, Section 301 § 3544(b), 44 U.S.C. § 3544(b).

[23] OMB M-10-15, supra, Frequently Asked Questions, Question 36, page 13.

responsible for ensuring appropriate security controls.[24] Agencies must also develop policies for information security oversight of contractors and other users with privileged access to Federal data.[25] In addition, FISMA requirements must be included in contracts and, when applicable, in grant terms and conditions.[26]

We determined that SSA's Contractor System oversight program generally complied with FISMA requirements for FY 2010. SSA's Contractor System oversight policy and procedures are contained in several documents. SSA's *Certification and Accreditation Handbook* contains the required security tasks that apply to all systems including Contractor Systems. SSA's *Interconnection Approval Process Guide* provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by non-SSA entities. SSA is also required to include the Federal security training and privacy requirements in all its services contracts.[27]

Although SSA has a Contractor Oversight process, we identified some areas that needed improvement. SSA lacks an Agency level contractor oversight policy in its Information System Security Handbook to provide comprehensive guidance. In addition, SSA policy does not require that contract terms include all FISMA requirements. We also found the following two issues with SSA's Contractor System oversight program.

SSA's Master System Inventory Contained All Systems But Did Not Identify Contractor Systems. In FY 2010, we found three systems that met the definition of systems "operated on the Agency's behalf by contractors or other entities" but not identified as such in SSA's master inventory. These systems are Access to Financial Institutions (AFI), operated by Accuity Inc.;[28] E2 Solutions, operated by the General Services Administration;[29] and Cyber Security Assessment and Management (CSAM),[30] operated by the Department of Justice.

[24] OMB M-10-15, supra, Frequently Asked Questions, Question 36, page 14.

[25] Id.

[26] OMB M-10-15, supra, Frequently Asked Questions section, Question 39, page 16.

[27] *Social Security Administration's Acquisition Handbook,* Section 0402 *Federal Information Security Management Act (FISMA) and Agency Privacy Management,* October 2008*.*

[28] AFI is an electronic process to automatically verify financial account balances alleged by claimants and beneficiaries during the Supplemental Security Income claims and redeterminations processes.

[29] E2 Solution is the travel system adopted by SSA.

[30] CSAM is SSA's FISMA tracking tool. CSAM enables the Agency and SSA's C&A Managers to gather system information and to create reports to support the FISMA assessment. SSA also uses CSAM for managing the identified weaknesses.

SSA Did Not Ensure that All Contractor Systems Met FISMA Requirements Before Putting Them Into Operation. Agencies are required to provide security protections for Contractor Systems.[31] SSA had taken some steps to ensure that E2 Solutions and CSAM had proper security controls. However, for AFI, SSA did not ensure the contractor system met FISMA requirements before putting it into operation.

OMB FISMA guidance states, "Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract."[32] Agencies must ensure all Contractor Systems have identical security procedures as its own systems.[33] For example, annual reviews, risk assessments, security plans, control testing, contingency planning and security authorization (C&A) must, at a minimum, explicitly meet NIST guidance.[34]

Accuity, Inc., has been a service provider to SSA since 2003. In 2003, SSA contracted with Accuity, Inc., to create a Web-based system that allowed Agency offices to electronically submit and receive Supplemental Security Income asset information.[35] SSA conducted a limited proof of concept in 20 field offices in New York and New Jersey in FY 2004. In FY 2005, SSA conducted a pilot in all 110 field offices in the 2 States. In November 2007, SSA decided to expand the system to California. In September 2010, SSA expanded the pilot once again to 14 additional States. The AFI application stores PII information. See Table 1 below.

Table 1: AFI Information Types

Representative Payee Information
Income Information
Personal Identity and Authentication Information
Entitlement Event Information
Payments Information
General Retirement and Disability Information
Reporting and Information
Survivor Compensation Information

[31] Pub. L. No. 107-347, Title III, Section 301 § 3544(b), 44 U.S.C. § 3544(b).

[32] OMB M-10-15, supra, Frequently Asked Questions section, Question 38, pages 14-15.

[33] Id.

[34] Id.

[35] This is referred to as the e4641 Asset Verification System. SSA contracted with Accuity Solutions in 2003 to develop the web-based system that automates the SSA-4641 consent form and handles the sending and receipt of bank account verifications. The system is owned by Accuity, Inc. The Form SSA-4641 is the *Authorization For The Social Security Administration To Obtain Account Records From A Financial Institution And Request For Records.*

Before expanding the AFI pilot to 14 additional States, the Agency

- conducted a System Security Categorization Review to determine the system impact level of AFI using federal guidance;[36]
- performed a Risk Assessment (RA) using penetration testing techniques; and
- obtained a Statement on Auditing Standards (SAS) 70 report on AT&T's Web hosting services.[37]

The RA did not examine all security controls as required by NIST; as a result, it may not have identified all security risks related to the AFI system. The AFI RA report listed only 87 of the 170 baseline security controls required by NIST for a moderate impact system.[38] Of the 87, 40 controls were assessed. Of the 40 controls assessed, 17 were physical security controls. The remaining 23 controls assessed resulted in13 security exceptions (1 high risk, 9 moderate risk, and 3 low risk) and more than a hundred of recommended security setting changes. Accuity and SSA addressed many of these security weaknesses immediately, but it is unclear what security risks SSA may be exposed to because of the security controls that were not assessed before the AFI pilot was expanded.

According to the OCIO, the AFI system is an important part of the agency's strategy to reduce improper payments and the expansion of the AFI pilot that occurred in September 2010 represented a critical milestone. The timeframe between contract award and pilot expansion did not permit a full security authorization to be performed. OCIO staff stated that SSA had taken a risk-based approach to obtain a level of assurance before expanding the AFI pilot given the short timeframe. SSA believes its approach is acceptable and compliant with the NIST guidance. Additionally, the Agency plans to complete a full C&A by the end of December 2010.

We agree that SSA did perform some security-related activities, but the Agency should have conducted a complete C&A or obtained C&A related information from other agencies doing business with Accuity before putting AFI into operation. To improve its contractor system oversight program, we recommend SSA

[36] The review used NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* and Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*. The categorization is derived from identifying the types of information stored or created in the system and determining the expected impact to SSA from a loss in confidentiality, integrity, and availability to the system or data.

[37] SAS No. 70, *Service Organizations*, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants. A service auditor's examination performed in accordance with SAS No. 70 represents that a service organization has been through an in-depth audit of its control objectives and control activities, which often include controls over IT and related processes.

[38] NIST *Special Publication 800-53, Revision 3, Online Database*, lists the minimum security control baselines for low-impact, moderate-impact, and high-impact information systems. AFI is a moderate impact system. There are 170 controls listed as the minimum control baseline for a moderate impact system. The impact level of a system is referred to the security categorization, see Footnote 36.

- establish a separate chapter in its Information System Security Handbook to outline all required security tasks for Contractor Systems Oversight according to OMB requirements;
- require that contracts include Federal security requirements;
- ensure compliance with Federal requirements and Agency policy for Contractor Systems Oversight; and
- complete the AFI C&A prior to further expanding AFI application to more States.

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Federal agencies must safeguard PII,[39] as required by the *Privacy Act of 1974*.[40] In addition, FISMA requires that agencies protect information collected or maintained by, or on behalf of, agencies commensurate with the risk and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction.[41] Further, OMB issued several memorandums[42] on how Federal agencies should safeguard PII.[43]

SSA has established policies and procedures for PII protection and requires that its employees be vigilant in safeguarding PII collected and maintained by the Agency in any format. However, we identified instances where SSA needed to improve its PII protection.

Our June 2010 report[44] stated SSA's Office of Disability Adjudication and Review's (ODAR) flexiplace[45] practices may have exposed claimant data to unauthorized disclosure.[46] ODAR allowed flexiplace employees to remove PII stored on

[39] See Footnote 12.

[40] Pub. L. No. 93-579, as amended, § 552a(e)(10), 5 U.S.C. § 552a(e)(10).

[41] Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A)(i), 44 U.S.C. § 3544(a)(1)(A)(i).

[42] OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006; M-06-16, *Protection of Sensitive Agency Information,* June 23, 2006; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007; and M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

[43] See Footnote 12.

[44] SSA OIG, *Controls Over the Flexiplace Program and Personally Identifiable Information at Hearing Offices* (A-08-09-19079), June 2010.

[45] Flexiplace allows qualified ODAR staff to perform assigned work at a management-approved alternate duty station, which is typically their personal residence. As such, employees who participate in Flexiplace take claimants' case files to their alternate duty stations. These case files can be in paper form or stored on portable devices, such as compact discs and laptop computers, and generally include claimants' PII.

[46] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, page 1, June 23, 2006, recommends that agencies encrypt all data on mobile computers/devices that carry agency data unless the data is determined to be non-sensitive. Agencies also need to 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.

unencrypted[47] compact discs. In addition, ODAR employees did not always comply with SSA's preventative controls, such as locking claimant PII, when traveling to, or working at, an alternate duty station. We also determined that ODAR did not always identify the removal, and confirm the return, of PII. We recommended that ODAR employees store electronic PII on an encrypted and password-protected laptop when working Flexiplace, until a compact disc encryption solution for ODAR is developed. Furthermore, we recommended that SSA reemphasize to ODAR employees the importance of complying with all Agency PII policies and directives and consider implementing additional procedures to account for the removal and return of PII.

In a November 2010 audit,[48] we reported computer hard drives awaiting disposal contained PII. In April 2009, our testing found these hard drives were not properly sanitized, as required by NIST[49] and SSA policy.[50] In addition, SSA could not account for the hard drives from some IT equipment awaiting disposal. These hard drives could potentially contain PII.

After we notified SSA of this issue, it reported the loss of these hard drives to the United States Computer Emergency Readiness Team (US-CERT). We made several recommendations to improve SSA's IT media sanitization policies and procedures. We recommended that SSA:

- designate one or more employees in each region who will certify and erase all information from IT media;
- test a representative sample of sanitized IT media to ensure all data and programs are effectively erased before disposal; and
- properly track IT media (that is, hard drives) through the sanitization and disposal process.

PROPER INCIDENT HANDLING AND NOTIFICATION

OMB requires that PII and unauthorized access related security incidents be reported to the US-CERT within 1 hour of discovery or detection.[51] In FY 2010, SSA reported

[47] Encryption is one method used to achieve security for data stored electronically. Encryption software converts data into a secret code so they are not easily understood, except by authorized users.

[48] SSA OIG, *The Social Security Administration's Controls for Ensuring the Removal of Sensitive Data from Excessed Computer Equipment* (A-14-10-11003), November 2010.

[49] FISMA requires compliance with information security standards promulgated under § 11331 of Title 40, which includes standards promulgated by NIST. Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(B)(i), 44 U.S.C. § 3544(a)(1)(B)(i). NIST recommends organizations sanitize information system media prior to disposal, release out of organizational control, or release for reuse. NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, Appendix F, page F-74.

[50] SSA, Information System Security Handbook, Section 10.3.1.

[51] OMB M-07-16, supra at page 10.

80 percent of the PII incidents to US-CERT within 1 hour. In FY 2009, SSA only reported 35 percent of PII incidents to US-CERT within 1 hour. SSA has made great strides to improve its PII incident reporting.

Our FY 2009 FISMA report found that SSA conducted additional research to confirm the PII incident actually occurred. Because SSA sometimes delayed reporting, valuable time was lost before law enforcement agencies and US-CERT were notified and could begin their investigation. Further, since SSA waited to confirm a PII incident instead of immediately reporting a suspected PII incident, the Agency did not comply with OMB policy.[52]

According to SSA, in FY 2010, the Agency revised its policy and no longer required additional research to confirm the PII incident actually occurred before reporting to US-CERT. SSA's new policy is consistent with OMB guidance.[53] In addition, the OCIO is implementing an automated PII Loss Reporting tool that will enable SSA to report higher percentage of PII incidents to US-CERT within 1 hour.

In FY 2009, we reported that SSA reported PII incidents to local law enforcement but not to our Office of Investigations. In FY 2010, we identified the same condition. FISMA requires that agencies notify and consult law enforcement agencies and their OIGs regarding security incidents, as appropriate.[54] SSA provided 19 PII incidents that it stated were reported to law enforcement. We tested a sample of five incidents, and found that SSA reported four and an SSA contractor[55] reported one to local law enforcement. However, our Office of Investigations did not receive any reports of PII incidents. Without receiving these referrals, the Office of Investigations could not determine whether these cases needed further investigation and therefore could not ensure SSA resolved these incidents in a timely manner to minimize PII exposure.

Further, SSA's Incident Response policy and procedures do not provide guidance on what type of security incidents, and in what timeframe these incidents, are required to be reported to the law enforcement and the OIG. NIST guidance states that one reason that many security-related incidents do not result in convictions is that organizations do not properly contact law enforcement.[56] "The incident response team should become acquainted with its law enforcement representatives before an incident occurs to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, and how it should be

[52] Id.

[53] OMB M-07-16, supra.

[54] Pub. L. No. 107-347, Title III, Section 301 § 3544(b)(7)(C)(i), 44 U.S.C. § 3544(b)(7)(C)(i).

[55] SSA could not provide documentation to support that the contractor reported the PII incident to local law enforcement because the contractor did not provide documentation to SSA.

[56] NIST SP 800-61, *Computer Security Incident Handling Guide*, Revision 1, Section 2.3.4.2, page 2-6, March 2008.

collected."[57] For PII incidents, SSA's policy reminds the component managers that they may need to take additional action, such as filing a report with IG. We believe the lack of guidance may have led to the findings discussed above.

We recommend SSA work with our Office of Investigations to establish policy and procedures on what types of PII incidents should be reported to law enforcement and the OIG and in what timeframes. As a result of these discussions, SSA should revise its PII reporting policy to document the types of PII incidents and timeframes that should be reported to law enforcement and OIG. In addition, we recommend SSA report all PII suspected or confirmed breaches of PII to US-CERT within 1 hour and to the OIG within established timeframes.

CONTINUED IMPROVEMENT IN CERTIFICATION AND ACCREDITATION PROCESS

SSA had conducted C&A reviews[58] for its 21 major systems and applications in the past 3 years, as required by FISMA.[59] To test SSA's compliance with OMB[60] and NIST[61] guidance, we reviewed four of the eight major systems or applications certified in FY 2010. We found SSA's C&A program generally met the requirements of NIST 800-37. However, we found SSA's Security Assessment process needed improvement.

As reported in our FY 2008 and 2009 FISMA reports, SSA's security assessments were largely based on less effective assessment methods, such as examinations and

[57] Id.

[58] According to NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

[59] OMB guidance states, "security authorizations are required for all Federal information systems." Section 3544(b)(3) of FISMA refers to "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems" and does not distinguish between major or other applications. OMB M-10-15, supra, Frequently Asked Questions, Question 25, page 9.

[60] Id.

[61] See Footnote 59.

interviews.[62] SSA made some improvements during the FY 2009 C&A process by significantly increasing the use of the test method[63] to assess the effectiveness of its security controls. However, we did not see any further improvement in this area in FY 2010. Our FY 2010 review continued to identify a low percentage of controls were assessed by hands-on testing.

There were weaknesses related to access control, configuration management, and other areas tested that should have been identified in the C&A review process. For example, GT's financial statement audit systems penetration and security testing identified weaknesses in patch management, password rules, configuration management and authentication.

We reiterate our FY 2009 recommendation that SSA continue to improve its C&A process by increasing the usage of the test assessment method.

CONTINUED IMPROVEMENT IN ITS CONTINGENCY PLANNING

In our FY 2009 FISMA report, we reported that SSA needed to improve its long-term and comprehensive IT Strategic Planning process to address its future processing needs, including its replacement project for the current National Computer Center (NCC). We also stated that SSA needed to address its ability to recover critical data processing operations in the event of disaster. We recommended that SSA use the second support center (SSC) as the disaster recovery site for the NCC.

In our 2010 Congressional Response Report: *The Social Security Administration's Disaster Recovery Capabilities* (Limited Distribution), we stated that SSA took steps to improve its disaster recovery capability. SSA accelerated the use of the SSC as a backup and recovery center and conducted an Accelerated Disaster Recovery Environment exercise to test the Agency's ability to recover completely from an NCC disaster. We also reported that SSA would be able to restore the Agency's mission-critical systems and non-mission-critical systems, with some gaps, should the NCC or SSC become unavailable.

Although SSA improved its Contingency Planning, the Agency's disaster recovery goal of 24 hours did not meet the Federal requirement of 12-hour recovery time.[64] The

[62] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* July 2008, page 9, defined 3 security control assessment methods: examine, interview and **test**. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects. The *interview* method is the process of conducting discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence. The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

[63] Id.

[64] FCD 1, *Federal Executive Branch National Continuity Program and Requirements*, February 2008, page 7, defines Primary Mission Essential Functions as those functions that need to be continuously performed during an event or resumed within 12 hours of an event, and that need to be maintained for up to 30 days after the event or until normal operations can be resumed.

Agency would be able to perform manual processes within the first 12 hours, but this would not meet the Federal Continuity Directive 1 (FCD 1) requirement. According to the FCD 1, an organization's continuity capacity (its ability to perform essential functions continuously), rests on key components and pillars, which are in turn built on the foundation of continuity planning and program management. The pillars are leadership, staff, communications and technology, and facilities.[65] FCD 1 states communications and business systems, including hardware and software for continuity operations should mirror those used in day-to-day business to assist continuity leadership and staff in a seamless transition to crisis operations.[66]

SSA reported that the Accelerated Disaster Recovery Environment exercise, which excluded systems and applications running at the SSC and systems that were redundant between the NCC and SSC, took 101hours (approximately 4 days) to recover SSA's mission-critical workloads. We recommend SSA continue improving its contingency planning and disaster recovery capacity to meet Federal requirements.

FULL IMPLEMENTATION OF ITS VULNERABILITY REMEDIATION POLICY

FISMA requires that agencies implement an agency-wide information security program that includes a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the Agency's information security policies, procedures, and practices.[67] OMB requires that agencies have a Plans of Actions and Milestones (POA&M) process to manage their remediation of security vulnerabilities.[68] In FY 2009, we reported that some of the deficiencies in the Agency's information security policies, procedures, and practices were not tracked by CSAM, and some Agency component quarterly remediation status reports were not provided to the OCIO. In FY 2010, SSA's components provided remediation status reports to the OCIO; however, SSA is still not tracking all information security deficiencies in CSAM.

We found that the POA&Ms for 11 high impact and 24 moderate impact security deficiencies were not tracked in CSAM. These deficiencies and related remediation plans were not tracked because SSA's Office of Telecommunications and Systems Operations did not report them to the OCIO. If the deficiencies are not reported and tracked, the OCIO has no assurance the security vulnerability has been remediated.

SSA should ensure all security deficiencies and their related remediation plans are timely reported and properly tracked in CSAM.

[65] FCD 1, supra, page 3.

[66] FCD 1, supra, page 4.

[67] Pub. L. No. 107-347, Title III, Section 301(b) § 3544(b)(6), 44 U.S.C. § 3544(b)(6).

[68] OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones,* October 17, 2001.

EMPLOYEES AND CONTRACTORS RECEIVE SECURITY AWARENESS AND SPECIALIZED SECURITY TRAINING

FISMA and OMB require that all agency personnel and contractors receive appropriate annual security awareness and specialized security training.[69] The Agency's policy stated that its approach to providing information security training to all SSA employees and systems users follows the guidelines in OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*,[70] which indicates that all individuals must be appropriately trained to fulfill their security responsibilities before they are granted access to agency systems. FISMA requires that each agency develop, document, and implement an agency-wide information security program.[71] NIST recommends agencies monitor the compliance and effectiveness of their security awareness training program.[72] An automated tracking system should be designed to capture key information regarding program activity (for example, courses, dates, audience, costs, and sources). The tracking system should capture the data at an agency level so they can be used to provide enterprise-wide analysis and reporting regarding awareness, training, and education initiatives.[73] In our FY 2009 FISMA review, we reported SSA's security awareness and training program had two deficiencies. These deficiencies were as follows.

1. SSA did not have an effective process to confirm that all users with log-in privileges completed annual security awareness training before accessing the Agency's systems.
2. SSA did not have an effective process to monitor compliance and effectiveness of the security awareness and specialized security training program.

In FY 2010, we continue to observe the same weaknesses. In addition, we identified that SSA's Security Awareness and Training policy did not provide guidance for determining the training needs for its employees with significant security

[69] OMB M-10-15, supra at page 15, states "…the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., user awareness training and training on agency policy and procedures)." Pub. L. No. 107-347, Title III, Section 301(b) § 3544(a)(4) requires each agency head to ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines. OMB M-07-16, Attachment 1 § A.2.d states, "Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties."

[70] Section A.3.a.2.b.

[71] Pub. L. No. 107-347, Title III, Section 301(b) § 3544(b), 44 U.S.C. § 3544(b).

[72] NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program*, October 2003, page ES-1 states, "Within agency IT security program policy, there must exist clear requirements for the awareness and training program."

[73] NIST SP 800-50, supra at section 6.1.

responsibilities.[74] Further, we could not test whether SSA's employees with significant IT security responsibilities had appropriate training because the Agency did not maintain documentation of such training. Without guidance for determining and documenting training needs, the Agency cannot ensure that employees with significant security responsibilities receive proper specialized security training for their job responsibilities.

SSA stated that all employees and contractor personnel received appropriate security awareness and specialized security training. However, in a sample of 30 employees with significant IT responsibilities, the Agency could only provide evidence that 24 employees received specialized training. We also found that 5 out of 20 new hires in our sample accessed SSA's systems before they received security awareness training.

We continue to recommend SSA develop a system or process that adequately confirms all users with log-in privileges complete annual security awareness training. Further, SSA needs to establish an automated tracking system to create, review, and maintain security awareness training records for all employees and contractors as evidence of compliance with OMB A-130, FISMA, and NIST guidelines.

In addition, we recommend SSA provide additional guidance for determining the training needs for its employees with significant security responsibilities and require retention of documentation for such training.

CONTINUOUS MONITORING PROGRAM STATUS FOR MEETING OFFICE OF MANAGEMENT AND BUDGET REQUIREMENT TREND

To date, SSA has complied with the OMB and NIST requirements for its continuous monitoring program. The continuous monitoring process consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this process is to provide ongoing oversight and monitoring of the security controls in the information system and inform the authorizing official when changes occur that may impact the system's security. The activities in this process are performed throughout the life cycle of the information system. Reaccreditation may be required because of specific changes to the information system or because Federal or agency policies require periodic reaccreditation of the information system.[75]

[74] SSA defined its employees with significant security responsibilities as "Employees with high levels of access to sensitive data who could affect agency-wide operations and/or who perform security, investigative, or auditing activities on a frequent basis. Personnel in these roles have significant access to sensitive information, such as social security records, medical records, business confidential documents, and other personally identifiable information, which needs to be protected against unauthorized access; fraudulent activities; and inappropriate disclosure and modification." SSA, Information Systems Security Handbook, Appendix H, *Security Training*.

[75] NIST SP 800-37, supra. NIST issued a revised guidance February 2010 and agencies have 1 year to fully implement the changes in the revised guidance.

In its FY 2010 FISMA guidance, OMB stated that “[a]gencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way…. Agencies need to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools.”[76] OMB also stated “any reporting should be a by-product of the agencies’ continuous monitoring programs and security management tool.”[77]

To meet OMB’s future continuous monitoring requirements, SSA reported it has procured consulting services to assist in developing a continuous monitoring strategy that includes evaluating the Agency’s current tools and methods in surveillance and external reporting. Per SSA, its contractor will identify existing technical solutions that provide near real-time capabilities that the Agency will be able to leverage for internal systems security decisions and external reporting. The contractor is also to recommend additional automated tools, procedures, and/or enhancements to maximize SSA’s capabilities to this end.

We commend SSA’s proactive efforts to develop a continuous monitoring program that meet or exceed OMB and NIST requirements. We encourage SSA to continue its efforts to meet OMB’s requirements in a timely manner.

CONCLUSIONS AND RECOMMENDATIONS

Based on the results of OIG and GT’s work, we determined that SSA’s security programs generally complied with FISMA; however, some improvements were needed. SSA continues to work with us to identify ways to comply with FISMA. The Agency continues to develop, implement, and operate security controls to protect its sensitive data, assets, and operations.

In our prior FISMA reports, we identified similar issues related to SSA’s (1) computer security program, (2) access controls, (3) strategic planning, (4) protection of PII, (5) vulnerability remediation process, (6) employee and contractor security awareness training, (7) incident reporting, and (8) C&A process. We affirm our prior recommendations in these areas and encourage the Agency to fully implement these recommendations.

[76] OMB M-10-15, supra at page 1.

[77] OMB M-10-15, supra at page 2.

SSA should continue to strengthen its overall security program and practices and ensure future compliance with FISMA and other information security related laws and regulations; therefore, we recommend SSA:

1. Continue to implement security controls to resolve the significant deficiency identified in this report.
2. Establish a separate chapter in its Information Systems Security Handbook to outline all required security tasks for Contractor Systems Oversight according to OMB requirements.
3. Require that contracts include Federal security requirements.
4. Ensure compliance with the Federal requirements and Agency's policy for Contractor Systems Oversight.
5. Complete the AFI C&A prior to further expanding AFI application to more States.
6. Work with the OIG Office of Investigations to establish policy and procedures on what types of PII incidents should be reported to law enforcement and the OIG and in what timeframes.
7. Revise its policy, guidance, procedures, and timeframes for reporting of PII incidents to law enforcement, including the OIG.
8. Ensure all PII incidents are reported to US-CERT and the OIG within the established timeframes.
9. Provide additional guidance for determining the training needs for its employees with significant security responsibilities, require retention of documentation for such training, and establish guidance to assess the effectiveness of its security training program.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

AFI	Access to Financial Institutions
C&A	Certification and Accreditation
Contractor System	Systems Operated on Agency’s Behalf by a Contractor or Other Entities
CSAM	Cyber Security Assessment and Management
FCD	Federal Continuity Directive
FISCAM	*Federal Information System Controls Audit Manual*
FISMA	*Federal Information Security Management Act of 2002*
FY	Fiscal Year
GT	Grant Thornton LLP
IG	Inspector General
IT	Information Technology
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODAR	Office of Disability Adjudication and Review
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SAS	Statement on Auditing Standards
SP	Special Publication
SSA	Social Security Administration
SSC	Second Support Center
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Appendix B

Office of the Inspector General Response to Annual *Federal Information Security Management Act of 2002* Reporting Inspector General Questions

Annual FISMA Reporting Inspector General Questions		
Agency Name: Social Security Administration		**Submission date: 11/15/10**
Section 1: Status of Certification and Accreditation Program		
1. Check one:	√	a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process. 2. Establishment of accreditation boundaries for agency information systems. 3. Categorizes information systems. 4. Applies applicable minimum baseline security controls. 5. Assesses risks and tailors security control baseline for each system. 6. Assessment of the management, operational, and technical security controls in the information system. 7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document. 8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.
		b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a certification and accreditation program.
Comments: SSA should continue to improve the effectiveness of its security assessments by increasing the number of controls assessed by the "test" method rather than the "interview" and "examine" methods.		
Section 2: Status of Security Configuration Management		
2. Check one:	√	a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for configuration management. 2. Standard baseline configurations. 3. Scanning for compliance and vulnerabilities with baseline configurations. 4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented. 5. Documented proposed or actual changes to the configuration settings. 6. Process for the timely and secure installation of software patches.

		b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a security configuration management program.

3. Identify baselines reviewed:	AIX 5.3 AIX 6.1 CA TopSecret 14 GA Checkpoint R70.1 CISCO IOS 12.2 CISCO IOS 12.3 CISCO IOS 12.4	HP-UX11 iSeries OS5 6 Juniper Netscreen 6.1.0r5.0 Oracle DB 11.1.0.7.3 Sun Solaris 8 Sun Solaris 9 Sun Solaris 10	USS 1.11 Windows XP Professional Windows Vista Enterprise Windows Server 2000 Windows Server 2003 z/OS1.11

Comments: Weaknesses were identified with SSA's software approval policies, and the Agency has not established baseline configurations for all environments.

We also identified network vulnerabilities during penetration testing, which the Agency has taken steps to remediate. In addition, we noted a design deficiency in the process to remediate rogue modems connected to the SSA network, and SSA's penetration testing identified systems/software not included in its inventory.

Section 3: Status of Incident Response & Reporting Program

4. Check one:	√	a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for responding and reporting to incidents. 2. Comprehensive analysis, validation and documentation of incidents. 3. When applicable, reports to US-CERT within established timeframes. 4. When applicable, reports to law enforcement within established timeframes. 5. Responds to and resolves incidents in a timely manner to minimize further damage.
		b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established an incident response and reporting program.

Comments: SSA can improve its incident response and reporting program by establishing additional guidance on reporting incidents to the OIG and law enforcement.

Section 4: Status of Security Training Program

5. Check one:	√	a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for security awareness training. 2. Documented policies and procedures for specialized training for users with significant information security responsibilities. 3. Appropriate training content based on the organization and roles. 4. Identification and tracking of all employees with login privileges that need security awareness training. 5. Identification and tracking of employees without login privileges that require security awareness training. 6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.
		b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a security training program.

Comments: SSA should provide additional guidance for determining the training needs for its employees with significant security responsibilities, require retention of documentation for such training, and establish guidance to assess the effectiveness of its security training program.		
Section 5: Status of Plans of Actions & Milestones (POA&M) Program		
6. Check one:	√	a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for managing all known IT security weaknesses. 2. Tracks, prioritizes and remediates weaknesses. 3. Ensures remediation plans are effective for correcting weaknesses. 4. Establishes and adheres to reasonable remediation dates. 5. Ensures adequate resources are provided for correcting weaknesses. 6. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POAM activities at least quarterly.
		b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a POA&M program.
Comments: We determined that not all POA&Ms were tracked in accordance with SSA's policy. Furthermore, SSA does not allocate resources to individual POA&Ms, rather, all security weaknesses needing resources are funded through its IT planning process. We also noted inconsistencies with POA&M identification and remediation dates.		
Section 6: Status of Remote Access Program		
7. Check one:	√	a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access. 2. Protects against unauthorized connections or subversion of authorized connections. 3. Users are uniquely identified and authenticated for all access. 4. If applicable, multi-factor authentication is required for remote access. 5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms. 6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives. 7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.
		b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a program for providing secure remote access.
Comments: We noted that SSA allowed flexiplace employees to remove personally identifiable information (PII) stored on unencrypted CDs. In addition, SSA did not confirm the return of PII after it was taken out of the office. Furthermore, SSA did not always remove PII from computer hard drives before disposal.		

		Section 7: Status of Account and Identity Management Program
8. Check one:	√	a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for account and identity management. 2. Identifies all users, including federal employees, contractors, and others who access Agency systems. 3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary. 4. If multi-factor authentication is in use, it is linked to the Agency's PIV program. 5. Ensures that the users are granted access based on needs and separation of duties principles. 6. Identifies devices that are attached to the network and distinguishes these devices from users. 7. Ensures that accounts are terminated or deactivated once access is no longer required.
		b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established an account and identity management program.
Comments: We identified weaknesses with SSA's process to ensure that accounts are terminated or deactivated once access is no longer required.		
		Section 8: Status of Continuous Monitoring Program
9. Check one:	√	a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for continuous monitoring. 2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc. 3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans. 4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.
		b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a continuous monitoring program.
Comments:		
		Section 9: Status of Contingency Planning Program
10. Check one:	√	a. The Agency established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

		2. The agency has performed an overall Business Impact Assessment. 3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures. 4. Testing of system specific contingency plans. 5. The documented business continuity and disaster recovery plans are ready for implementation. 6. Development of training, testing, and exercises (TT&E) approaches. 7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.
		b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.
		c. The Agency has not established a business continuity/disaster recovery program.
Comments: Although SSA's goal to restore primary mission essential functions within 24 hours does not meet Federal Continuity Directive 1's 12-hour requirement, SSA has taken steps to improve its disaster recovery capabilities.		
Section 10: Status of Agency Program to Oversee Contractor Systems		
11. Check one:	√	a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes: 1. Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines. 2. A complete inventory of systems operated on the Agency's behalf by contractors or other entities. 3. The inventory identifies interfaces between these systems and Agency-operated systems. 4. The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that is owns and operates. 5. The inventory, including interfaces, is updated at least annually. 6. Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.
		b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.
		c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.
Comments: SSA's inventory does not distinguish between Agency systems and systems operated on its behalf by contractors or other entities. In addition, we found one contractor system where SSA did not fully comply with the Federal requirements for contractor systems oversight.		

Background and Current Security Status

The *Federal Information Security Management Act of 2002* (FISMA) requires that agencies create protective environments for their information systems. It does so by creating a framework for annual information technology (IT) security reviews, vulnerability reporting, and remediation planning, implementation, evaluation, and documentation.[1] In Fiscal Year (FY) 2005, the Social Security Administration (SSA) resolved the long-standing internal controls reportable condition concerning its protection of information.[2] However, during the FY 2009 and 2010 financial statement audit, SSA's management of access to its systems was identified as a significant deficiency.[3] SSA continues to work with us and Grant Thornton LLP to further improve the security and the protection of information and information systems and resolve other issues observed during prior FISMA reviews.

In the FY 2010 FISMA guidance, OMB Memorandum M-10-15, OMB stated that agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way.[4] To do this, agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information. Agencies need to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools.[5] OMB also stated any reporting should be a by-product of

[1] Pub. L. 107-347, Title III, Section 301, 44 U.S.C. § 3544(a)(1), (a)(2), and (b)(1).

[2] SSA's FY 2005 *Performance and Accountability Report,* page 164.

[3] The definition **of a significant deficiency for financial statement internal control** is provided by the Statement on Auditing Standards No. 115 (SAS 115) *Communicating Internal Control-Related Matters Identified in an Audit.* SAS 115 states a significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. OMB provides the definition of **a significant deficiency under FISMA**. OMB M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* April 21, 2010, page 23 defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

[4] OMB Memorandum M-10-15, supra at page 1.

[5] Id.

the agencies' continuous monitoring programs and security management tool.[6] Agencies should provide direct feeds from their security management tools to CyberScope. For those agencies that do not have this ability, OMB will soon release a roadmap that will allow agencies to upload data from security management tools to CyberScope.[7]

For FY 2010, FISMA reporting for agencies through CyberScope will follow a three-tiered approach:[8]

1. Data feeds directly from security management tools.
2. Government-wide benchmarking on security posture.
3. Agency-specific interviews.

This year, OMB instructed the Inspectors General (IG) to focus on their respective agency's management performance, in line with the requirements of FISMA.[9] The IGs were asked to assess agency performance in 10 major FISMA programs[10] specified by OMB using pre-established key attributes for each program. IGs were also required to determine areas for significant improvement if any agency programs did not have these key attributes.[11] See details in Appendix B.

This report informs Congress and the public about SSA's security performance and fulfills OMB's requirement under FISMA to submit an annual report to Congress. It provides OMB an assessment of SSA's IT security strengths and weaknesses and a plan of action to improve performance. OMB requires that agencies use an automated tool, CyberScope, to submit the annual FISMA report.

[6] OMB Memorandum M-10-15, supra at page 2.

[7] Id.

[8] OMB Memorandum M-10-15, supra at pages 2-3.

[9] OMB M-10-15, supra at page 3.

[10] Id.

[11] The OMB-specified attributes for each program and the significant improvement examples are posted on OMB's CyberScope Website. The agency Chief Information Officers and IGs all report through CyberScope.

Scope and Methodology

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency's Office of Inspector General (OIG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security program and practices, as well as a review of an appropriate subset of agency systems.[1] We contracted with Grant Thornton LLP (GT) to audit the Social Security Administration's (SSA) Fiscal Year (FY) 2010 financial statements. Because of the extensive internal control system work that is completed as part of that audit, our FISMA review requirements were incorporated into the GT financial statement audit contract. This evaluation included *Federal Information System Controls Audit Manual* (FISCAM) level reviews of SSA's financial related information systems. GT performed an "agreed-upon procedures" engagement using FISMA, Office of Management and Budget (OMB) Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, National Institute of Standards and Technology guidance, FISCAM, and other relevant security laws and regulations as a framework to complete the OIG-required review of SSA's information security program and practices and its information systems.

The results of our FISMA evaluation are based on our FY 2010 financial statement audit and working papers related to its agreed-upon procedures engagement as well as various audits and evaluations performed by this office and other entities. We also reviewed the final draft of the Chief Information Officer 2010 Annual FISMA Report.

Our evaluation followed OMB's FY2010 FISMA guidance and focused on the following SSA programs: Certification and Accreditation, Configuration Management, Security Incident Management, Security Training, Remediation/ Plans of Action and Milestones, Remote Access, Identity Management, Continuous Monitoring, Contract Oversight and Contingency Planning.

We performed field work at SSA facilities nationwide from March to November 2010. We considered the results of other OIG audits performed in FY 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] Pub. L. No. 107-347, Title III, section 301(b), 44 U.S.C § 3545 (a)(1), (a)(2), and (b)(1).

The Social Security Administration's Certified and Accredited Systems

	System	Acronym
	General Support Systems	
1	Audit Trail System	ATS
2	Comprehensive Integrity Review Process	CIRP
3	Death Alert, Control and Update System	DACUS
4	Debt Management System	DMS
5	Enterprise Wide Mainframe & Distributed Network Telecommunications Services System	EWANS
6	FALCON Data Entry System	FALCON
7	Human Resources Management Information System	HRMIS
8	Integrated Client Database	ICDB
9	Integrated Disability Management System	IDMS
10	Quality System	QA
11	Security Management Access Control System	SMACS
12	Social Security Online Accounting & Reporting System	SSOARS
13	Security Unified Measurement System	SUMS
	Major Applications	
1	Electronic Disability System	eDib
2	Earnings Record Maintenance System	ERMS
3	National Investigative Case Management System	NICMS
4	Recovery of Overpayments, Accounting and Reporting System	ROAR
5	Retirement, Survivors, & Disability Insurance Accounting System	RSDI ACCTNG
6	Supplemental Security Income Record Maintenance System	SSIRMS
7	Social Security Number Establishment and Correction System	SSNECS
8	Title II System	Title II

Appendix F

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Grace Chi, Acting Audit Manager

Acknowledgments

In addition to the persons named above:

Tina Nevels, Auditor

Michael Zimmerman, Auditor

For additional copies of this report, please visit our Website at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-10-20109.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

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, House of Representatives

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

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

Chairman and Ranking Minority Member, Committee on Commerce, Science and Transportation, U.S. Senate

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

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts 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 reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations 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 liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG 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. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.