FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2008 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act

September 2008 **A-14-08-18063**

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 19, 2008 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2008 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-08-18063)

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) 2008.[1]

BACKGROUND

FISMA provides the framework for securing the Government's information and information technology (IT). All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the effectiveness of their security programs. FISMA requires that each agency develop, document and implement an agencywide 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 FY 2008 FISMA guidance on July 14, 2008.[3]

SCOPE AND METHODOLOGY

FISMA directs each agency's Office of Inspector General (OIG) to perform an annual, independent evaluation of the effectiveness of the agency's information security program and practices.[4] We contracted with PricewaterhouseCoopers, LLP (PwC) to

---

[1] Pub. L. No. 107-347, Title III, Section 301 *et seq.,* 44 U.S.C. § 3541 et *seq*.

[2] Pub. L. No. 107-347, Title III, Section 301 (b)(1) § 3544 (b), 44 U.S.C. § 3544 (b).

[3] OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 14, 2008.

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

audit SSA's FY 2008 financial statements.[5] Because of the extensive internal control system review that is completed as part of that audit, the OIG FISMA requirements were incorporated into the PwC financial statement audit contract. This evaluation included reviews of SSA's mission-critical sensitive systems, as described in the Government Accountability Office's *Federal Information System Controls Audit Manual (FISCAM)*. PwC used FISMA, OMB guidance,[6] National Institute of Standards and Technology (NIST) guidance, FISCAM, and other relevant security laws and regulations as a framework to complete the required OIG review of SSA's information security program and its sensitive systems. In June 2008, the President's Council on Integrity and Efficiency (PCIE) issued a white paper[7] related to the protection of Personally Identifiable Information (PII), OIG access to records, and key escrow management. In August 2008, we informed SSA that we would include an assessment of these issues in our FISMA work since they are intrinsically related to FISMA requirements. See Appendix D for more details on the Scope and Methodology.

SUMMARY OF RESULTS

Based on the results of OIG's and PwC's audit work, we determined that SSA substantially met the FISMA requirements for FY 2008. SSA continues to work towards maintaining a secure environment for its information and systems and has made improvements since FY 2007 to strengthen its compliance with FISMA. For example, SSA continues to have sound remediation, certification and accreditation (C&A), and inventory processes. In FY 2008, SSA completed an inventory of its 20 major systems and over 300 subsystems. Our review found the FY 2008 inventory was accurate and complete.

SSA also maintained C&A for all 20 major systems and conducted re-certifications of 4 major systems using NIST Special Publication (SP) 800-37 guidance.[8] Over the past 3 years, we have reviewed all 20 C&As for the major systems, and they were substantially compliant with NIST SP 800-37. We reviewed SSA's Plans of Action and Milestones (POA&M) process, inventory process and overall security program. See Appendix E for the complete list of major systems and applications that have been certified and accredited.

---

[5] OIG Contract Number GS-23F-0165N, March 16, 2001. FY 2008 option was exercised on November 26, 2007.

[6] See footnote 3.

[7] PCIE Information Technology Investigations Sub-Committee Report, *Key Escrow Management and File Encryption Challenges for the Federal Inspector General Community*, June 2008.

[8] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

Even though we noted several areas that would enhance security of SSA's systems and sensitive information, these issues do not rise to the level of non-compliance with FISMA requirements either collectively or individually. SSA should ensure

- adequate protection of PII;
- the C&A process and the systems inventory are robust and complete to support a sound information security program;
- the POA&M process appropriately maintains and monitors the remediation of deficiencies;
- implementation of effective system access controls; and
- all employees and contractors receive security awareness and specialized training.

During our FISMA review, nothing came to our attention that warranted further action related to the PCIE's recommendations at this time.

SSA'S EFFORTS TO PROTECT PII

Over the past several years, OMB has issued guidances on safeguarding PII and has included specific reporting requirements in the annual FISMA guidances. The current FISMA guidance[9] requires that agencies include the following items in an appendix to their annual FISMA report:

- a breach notification policy;
- an implementation plan and progress to eliminate unnecessary use of Social Security numbers (SSN);
- an implementation plan and progress update on review and reduction of holdings of PII; and
- a policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

SSA has included these four PII-related items in its FY 2008 FISMA submission. SSA has created a website for employees that explains responsibilities, polices and procedures for protecting PII. The website contains *Policy and Procedures for All SSA Employees for Reporting the Loss or Suspected Loss of Personally Identifiable Information*. In addition to training for employees, SSA is working to eliminate unnecessary use of the SSN and reduce holdings of PII. The Agency has a policy outlining rules of behavior[10] but needs to improve Agency-wide procedures to ensure better identification of violations and consistent actions taken against the violators. Stronger procedures will likely result in more consistent and appropriate handling of

[9] OMB M-08-21, supra at cover page.

[10] Information Systems Security Handbook (ISSH), *Rules of Behavior for Users and Managers of SSA's Automated Information Resources,* March 23, 2001.

violations and improve the effectiveness of the rules of behavior as a deterrent for inappropriate activity.

The Agency has also established a PII Executive Steering Committee (ESC), which provides oversight and recommendations on SSA policy, and the PII Breach Response Group whose role is to engage in Agency planning in the event of a breach. While the OIG has been included as a member in the PII Breach Response Group, it has not been invited to fully participate in critical meetings. Similarly, OIG has not been included in the PII ESC, as recommended by OMB.[11] By allowing the OIG to participate to the fullest extent feasible in these groups, SSA will be better able to respond to data losses.

While SSA has taken numerous steps to protect PII, OIG audit work completed during FY 2008 identified areas that could be improved. When developing its plan to reduce unnecessary use of SSNs, SSA should consider a cross-section of potential SSN uses. For example, SSA should consider information currently sent to disability determination services (DDS) contractors providing services to beneficiaries and ensure contractors are only receiving information they need to know. Additionally, one of our audit reports found that SSA's publication of the Death Master File (DMF) has resulted in the breach of PII. Each year SSA adds 2.5 million death records in the DMF that SSA publishes to the public with 99.59 percent accuracy rate. Our audit was limited to data between January 2004 and April 2007 and found over 20,000 living individuals erroneously listed as deceased on the DMF and their PII exposed.[12] The OMB requirement for Agencies to report PII incidents to U.S. Computer Emergency Readiness Team (US-CERT) was issued in July 2006.[13] SSA has begun to notify US-CERT and is conducting a risk assessment to determine how to best inform the individuals erroneously listed in the DMF. SSA has also implemented different methods and explored ways to reduce the error cases. SSA should continue to ensure that these types of situations are addressed in its plan to reduce the unnecessary use of SSNs. As SSA strives to safeguard the PII in its possession, it needs to continue to assess and enhance policies and procedures.

SSA'S CERTIFICATION AND ACCREDITATION PROCESS AND SYSTEM INVENTORY

SSA conducted C&As for each of the 20 major systems, at least every 3 years, in accordance with NIST Special Publication 800-37. We have cumulatively reviewed the 20 C&As for the major systems over the past 3 years. SSA's C&A process is

---

[11] OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification,* September 20, 2006, attachment, page 2 and OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007, page 1.

[12] OIG Report, *Personally Identifiable Information Made Available to the General Public Via the Death Master File* (A-06-08-18042), May 2008.

[13] 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. This Memorandum requires agencies to report PII related incidents to US-CERT within 1 hour of the discovery of the incident.

substantially compliant with FISMA and NIST requirements and standards. However, we did note several areas where SSA could improve its C&A process.

Our review of documentation showed that SSA's security assessment and evaluation met the NIST security assessment requirements. However, SSA's assessments were largely based on examinations and interviews. We recommend that SSA increase the depth of testing its security controls. In each of the C&A documentation packages we reviewed this year, only limited security controls of the systems were "tested."[14] In our opinion, additional in-depth testing of its security controls and program would give SSA more assurance of the soundness of its security program, particularly in light of the rapid changes in the information security field. For example, SSA's security control assessment did not identify several security weaknesses in its general supporting system that were identified by PwC's security testing performed during the FY 2008 Financial Statement audit.

SSA could enhance the documentation of risk remediation results and residual risk in its C&A packages, as recommended by NIST.[15] We did not find a list of POA&Ms for some of the C&A security findings nor did we find clear documentation of residual risk for the systems reviewed. Based on our discussion with Agency personnel, SSA is considering improving the documentation of the system's residual risk and will ensure all POA&Ms are properly documented.

During our audit, we examined the completeness of SSA's FY 2008 System Inventory by conducting comparison and analysis, reviewing numerous documents and holding discussions with Agency personnel regarding SSA's annual System Inventory process. We did note a few subsystems listed in the C&As and other documentation that were not included in SSA's official inventory for FY 2008. The Agency added these to the inventory. We are not aware of any other omissions. As a result, we concluded that SSA's System Inventory includes more than 96 percent of the Agency's major systems and subsystems and were covered by the C&A process. However, SSA should ensure consistency between its C&A documentation and official system inventory.

SSA'S PLAN OF ACTION AND MILESTONES PROCESS

OMB FISMA guidance states that the purpose of a POA&M process is to identify and track all IT system security weaknesses in one central location.[16] SSA has designated

---

[14] 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 to compare actual with expected behavior.

[15] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002, page 40, defined Residual Risk as "The risk remaining after the implementation of new or enhanced controls is the residual risk."

[16] OMB M-08-21, supra, question 34 at page 13.

the Office of the Chief Information Officer (OCIO) as the responsible component. OCIO uses the Automated System Security Evaluation and Remediation Tracking (ASSERT) software to monitor and report on IT security weaknesses. OCIO also uses ASSERT to support the POA&M process that tracks identified IT security weaknesses through the correction or remediation of these weaknesses.

We found that SSA ASSERT tool was implemented as an Agency-wide tool. However there are areas that need improvements. We tested 20 security weaknesses that should be included in ASSERT to test its completeness. We did not find 4 of the 20 weaknesses and its POA&M. We also noted the OCIO had experienced difficulties receiving all reports on IT security weaknesses. Increased coordination between OCIO and security components would improve the POA&M process.

The Agency has made progress and continues to improve its policies and procedures to ensure all IT security weaknesses are appropriately included in the tracking and remediation processes. The Agency needs to ensure it complies with and fully implements these policies and procedures.

IMPLEMENTATION OF SYSTEM ACCESS CONTROLS

Controlling and limiting 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 IT resources. Over the years, SSA has worked to establish sufficient access controls as evidenced by the use of Top Secret software and the System Security Profile Project. As a result, in FY 2005, the access control issue was removed as a reportable condition from SSA auditors' financial statement report. However, we noted instances where SSA's access controls could be strengthened.

For example, some programmers had excessive access to production data of certain SSA systems. SSA should ensure that individuals only have access to the systems that are necessary for them to perform their duties. Another area involved access to sensitive data held by DDS employees.[17] These are State employees who perform services for SSA and periodically need to access SSA records.

[17] OIG report, *Access to Social Security Administration Data Provided by Disability Determination Services Positional Profiles* (A-14-07-17024), September 28, 2007.

We found that

- some DDS employees were granted unneeded access to SSA's sensitive data;
- access control software did not suspend access after a period of non-use if the default password had never been changed; and
- access needs for each resource contained in the DDS profiles had not been documented for DDS employees.

Our audit work, in FYs 2007 and 2008, observed a need to strengthen employment suitability checks of SSA contractor personnel. We found that a number of contractor staff did not receive background checks.[18] Therefore, these individuals should not have been permitted to work at an SSA facility or have physical access to Agency hardware or facilities that may contain program or sensitive information. As a result, SSA may be exposing its sensitive data to possible compromise. SSA should continue to work to strengthen access controls in both of these areas.

SECURITY AWARENESS AND SPECIALIZED TRAINING FOR EMPLOYEES AND CONTRACTOR PERSONNEL

Security Awareness and Specialized Security Training for Agency Personnel and Contractors.

SSA needs to ensure that all Agency personnel and contractors receive security awareness training. OMB guidance states that all Agency and contractor personnel have security awareness training each year.[19] Historically, all SSA employees have been receiving some form of security awareness information and annually signed that they read SSA's security awareness policies. This year, our testing showed that, while most SSA personnel had received security awareness, SSA could not provide documentation for all individuals.

SSA requires that all contractor personnel read and sign annual statements that they completed SSA's security awareness training. This year, the Agency implemented a process of centrally maintaining and monitoring the security awareness efforts for its contractors. However, over 20,000 of 22,000 contractors did not receive any security awareness training. For example, some of the contractors who did not receive security awareness training were individuals assigned to install hardware on SSA's network.[20]

---

[18] OIG Report, *The Social Security Administration's Information Technology Maintenance and Local Area Network Relocation Contract* (A-14-07-17022), May 21, 2007; OIG Report, *The Social Security Administration's Consulting Service Contract for the Time Allocation System* (A-14-08-18020), August, 2008; and OIG Report, *The Social Security Administration's Enterprise-wide Network Infrastructure Contract* (A-14-08-18014), September, 2008.

[19] OMB M-08-21, supra, question 43 at page 26.

[20] OIG Report, *The Social Security Administration's Enterprise-wide Network Infrastructure Contract* (A-14-08-18014), September, 2008.

Identifying Individuals with Significant IT Security Responsibilities

According to FISMA, agencies are required to ensure that employees and contractor personnel with significant IT security responsibilities receive security awareness and specialized training.[21] Meeting this requirement involves two steps: identifying individuals who have significant IT security responsibilities and ensuring these people receive specialized training.

In 2007, SSA developed and implemented a clear definition for the employees with significant IT security responsibilities.[22] Our 2007 review noted numerous employees that seemed to fit the description; however, the Agency did not identify them as having significant IT responsibilities. This year, we observed a significant improvement in SSA's effort to identify employees and contractors with significant IT responsibilities.

During our review of specialized training, we noted one area related to SSA's physical security and overall IT security that the Agency still needs to address. Our testing noted a small number of employees and contractors who were involved with the implementation of Homeland Security Presidential Directive (HSPD) 12[23] who were not identified by SSA as having significant IT responsibilities[24] and therefore did not receive any specialized training. SSA needs to ensure appropriate security training is provided to Agency and contractor personnel with significant IT security responsibilities. SSA has the ultimate responsibility to ensure those who could impact its systems have sufficient security awareness and specialized training.

---

[21] Pub. L. No. 107-347, Title III, Section 301 (b)(1) § 3544 (a)(3)(D), 44 U.S.C. § 3544 (a)(3)(D).

[22] SSA's ISSH Appendix H states;" 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."

[23] HSPD-12 mandates the development of a common identification standard for Federal employees and contractors.

[24] ISSH, Appendix H, *Security Training*.

KEY ESCROW MANAGEMENT AND FILE ENCRYPTION CHALLENGES

In June 2008, the PCIE issued a white paper[25] to all Inspectors General regarding concerns related to protection of PII, OIG access to records, and key escrow management.[26] Recommendations were made to OIGs on how to better secure protection of PII based on OMB requirements. These recommendations addressed the following areas.

1. Diligent protection of sensitive PII and implementation of appropriate information security controls.
2. Ensuring OIG access to all (including contractor) records, reports, audits, reviews, documents, papers, recommendations, or other material available to accomplish its programs and operations.
3. Prevention of commingling of Federal data at contractors that store SSA data.
4. Establishment of a key management policy that describes the goals, responsibilities, and overall requirements for the management of cryptographic keying material used to protect private or critical facilities, processes, or information.

While these issues are not expressly discussed in OMB's FY 2008 FISMA guidance, they are closely related to the intent of FISMA and OMB's emphasis on the protection of PII. During our FISMA review, nothing came to our attention that warranted further action related to the PCIE's recommendations at this time. To improve processing in these areas, SSA is expanding policies and procedures for key escrow management, file encryption, and standardized contract language.

CONCLUSIONS AND RECOMMENDATIONS

During our FY 2008 FISMA evaluation, we determined that SSA substantially met the requirements of FISMA. SSA worked cooperatively with the OIG to identify ways to comply with FISMA. SSA continues to operate a myriad of security controls to protect its sensitive data, assets, and operations. SSA develops new policies and procedures when required.

---

[25] PCIE Information Technology Investigations Sub-Committee white paper, *Key Escrow Management and File Encryption Challenges for the Federal Inspector General Community*, June 2008.

[26] Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow by a third party so that, under certain circumstances, an authorized third party may gain access to those keys.

To continue to strengthen SSA's overall security program and practices and to ensure future compliance with FISMA and other information security related laws and regulations, we recommend SSA ensure:

1. Controls to protect PII, including reporting loss of PII, are fully implemented in accordance with OMB guidances.
2. Sufficient testing of security controls in the C&A process to fully identify system security weaknesses.
3. All C&As are properly and consistently prepared and include risk remediation results and residual risk documentation.
4. All systems and subsystems documented in the C&A package are consistent with SSA's official system inventory.
5. All IT security weaknesses are timely reported to OCIO and properly recorded and monitored in the POA&M system.
6. System access controls are fully implemented to meet least privilege criteria for all users of SSA's systems.
7. All Agency and contractor personnel receive annual security awareness.
8. All Agency and contractor personnel with significant IT responsibility receive specialized training.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

ASSERT	Automated System Security Evaluation and Remediation Tracking
C&A	Certification and Accreditation
DDS	Disability Determination Services
DMF	Death Master File
ESC	Executive Steering Committee
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IT	Information Technology
ISSH	Information Systems Security Handbook
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PCIE	President's Council in Integrity and Efficiency
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
POA&M	Plan of Action and Milestones
PwC	PricewaterhouseCoopers LLP
SP	Special Publication
SSA	Social Security Administration
SSN	Social Security Number
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Office of the Inspector General's Completion of the Office of Management and Budget Questions Concerning the Social Security Administration's Compliance with the Federal Information Security Management Act

Section C Inspector General: Question 1 and 2

Agency Name: Social Security Administration **Submission date: 9/19/08**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)	
Social Security Administration	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed
Agency Totals	High	0	0	0	0	0	0
	Moderate	8	8	0	0	8	8
	Low	12	12	0	0	12	12
	Not Categorized	0	0	0	0	0	0
	Total 20		**20**	**0**	**0**	**20**	**20**

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

Question 2 : Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Social Security Administration	**FIPS 199 System Impact Level**	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
	High	0	0.0	0	0.0	0	0.0
	Moderate	8	40.0	8	40.0	8	40.0
	Low	12	60.0	12	60.0	12	60.0
	Not Categorized	0	0.0	0	0.0	0	0.0
Agency Totals	**Total 20**		**100.0**	**20**	**100.0**	**20**	**100.0**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	N/A. SSA does not use any systems that are controlled or managed by contractors or other organizations
3.b.	**The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	Approximately 96-100% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency-owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY 2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.	N/A

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process		
Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided. For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status. - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time		
4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Almost Always, for example, approximately 96-100% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Almost Always, for example, approximately 96-100% of the time
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	- Mostly, for example, approximately 81-95% of the time
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Mostly, for example, approximately 81-95% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 96-100% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time
POA&M process comments: 4c & 4d. Agency should improve its monitoring process to ensure that all findings are included in the process. SSA needs to ensure that all appropriate issues from the Financial Statement audit and low risk recommendations are accurately tracked.		

Question 5: IG Assessment of the Certification and Accreditation Process			
Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.			
5.a.	The IG rates the overall quality of the Agency's certification and accreditation process as: Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Good	
5.b.	The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)	Security plan	√
		System impact level	√
		System test and evaluation	√
		Security control testing	√
		Incident handling	√
		Security awareness training	√
		Configurations/patching	√
		Other:	
C&A process comments: SSA should enhance C&A testing to fully identify security weaknesses.			

Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
6	Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question # 5 (SAOP reporting template), including adherence to existing policy, guidance, and standards. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Excellent
Comments:		
7	Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Excellent
Comments: While the Agency has made excellent progress to improve its protection of PII, there are areas the Agency could improve. For example, the Agency needs to ensure the OIG is an active participate in workgroups chartered to protect PII.		
Question 8: Configuration Management		
8.a.	Is there an agency-wide security configuration policy? Yes or No.	Yes
Comments: SSA does have agency-wide security configuration policies. However, SSA does not have a procedure in place to monitor compliance with its Oracle configuration policy. Problems with Oracle configuration were noted during the security testing of FY 2008 Financial Statement Audit.		

8.b.	Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available form the National Institute of Standards and Technology's website at http://checklists.nist.gov. Response categories: Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Almost Always- for example, approximately 96-100% of the time
8.c.	Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2. New Federal Acquisition regulation 2007-004 language, which modified "Part 39-Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	No
	c.3. All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	Yes
Comments: The Agency has an XP risk model and is monitoring compliance with the risk model. The Agency does not currently have any VISTA systems in production.		

Questions 9,10, and 11		
Question 9: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to the US-CERT. Yes or No. (http://www.us-cert.gov)	Yes
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments: SSA needs to improve its reporting of incidents. One of our audit reports found that SSA's publication of the Death Master File (DMF) erroneously included living individuals' PII and thereby resulted in the breach of PII. The audit was limited to data between January 2004 and April 2007 and found over 20,000 living individuals erroneously listed as deceased on the DMF and their		

PII exposed. In May 2008, SSA began notifying US-CERT. SSA is performing a risk analysis to assess any impact on individuals and is planning to develop a notification policy.	
Question 10: Security Awareness Training	
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees	Frequently- or approximately 71-80% of employees
Comments: Our review showed that 58,022 SSA employees signed annual statements that they had read SSA's security awareness policies. Additionally, 1,607 contractors received security awareness training. Therefore, we confirmed that 59,629 out of 83,925 employees and contractors or 71% received security awareness.	
Question 11 Collaborative Web Technologies and Peer-to-Peer File Sharing	
Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	Yes
Question 12 E-Authentication Risk Assessments	
12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.	Yes
12.b. If the response is "No", then identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	SSA did identify all e-authentication applications. Nothing came to our attention to indicate that the Agency did not validate all e-authentication applications. Validation may include a wide-range of activities such as interviews, desk reviews, and automated testing. SSA would benefit by using the highest level of validation testing to ensure the security of its e-authentication application.

Background and Current Security Status

The *Federal Information Security Management Act* (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 longstanding internal control reportable condition concerning its protection of information.[2] SSA continues to work with the Office of the Inspector General and PricewaterhouseCoopers LLP to improve security over the protection of information and resolve other issues observed during prior FISMA reviews.

The Office of Management and Budget (OMB) continues to stress the importance of protecting the public's privacy and Personally Identifiable Information (PII) as emphasized by new guidance, such as OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. This new guidance mandates agencies increase efforts to reduce the use of PII collected and held. OMB is incorporating more privacy and PII protection questions in its annual FISMA guidance. OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 14, 2008 requires agencies to include in their annual FISMA submission the following items:

- a breach notification policy;
- an implementation plan and progress update to eliminate unnecessary use of Social Security numbers;
- an implementation plan and progress update on the review and reduction of holdings of PII; and
- a policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

In addition, OMB Memorandum M-08-21 requires that Inspectors General rate the quality of agencies' Privacy Impact Assessment process and progress on implementing OMB Memorandum M-07-16.

[1] Pub. L. No. 107-347, Title III, Section 301 *et seq,,* 44 U.S.C. § 3541 *et seq*.

[2] SSA's FY 2005 *Performance and Accountability Report,* page 163.

This report informs Congress and the public about the Federal Government's security performance, and fulfills OMB's requirement under FISMA to submit an annual report to Congress. It provides OMB's assessment of Government-wide IT security strengths and weaknesses and a plan of action to improve performance. The Committee on Oversight and Government Reform issues an annual *Report Card on Computer Security at Federal Departments and Agencies*. SSA has received a score of A+ and A over the past 2 years.

Scope and Methodology

The *Federal Information Security Management Act* (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] The Social Security Administration's (SSA) OIG contracted with PricewaterhouseCoopers LLP (PwC) to audit SSA's Fiscal Year (FY) 2008 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 PwC financial statement audit contract. This evaluation included Federal Information System Controls Audit Manual (FISCAM) level reviews of SSA's mission-critical sensitive systems. PwC performed an "agreed-upon procedures" engagement using FISMA, the Office of Management and Budget (OMB) Memorandum M-08-21, *FY 2008 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 sensitive systems. We also considered the security implications of OMB Memorandum M-07-16.

The results of our FISMA evaluation are based on the PwC FY 2008 *Independent Accountants' Report on Applying Agreed-Upon Procedures* report and working papers and various audits and evaluations performed by this office. We also reviewed the final draft of *SSA's FY 2008 Security Program Review as required by the Federal Information Security Management Act*.

Our major focus was an evaluation of SSA's plan of action and milestones (POA&M) process, risk models and configuration settings, certifications and accreditations (C&A), and systems inventory processes. Our evaluation of SSA's POA&Ms included an analysis of Automated Security Self-Evaluation and Remediation Tracking system and its policies. Our review of the Agency's C&A process included an analysis of the C&As for each of the 20 major systems. We also reviewed SSA's updated systems inventory and the policy for the update processes. In addition, we considered the impact of related OIG FY 2008 audits.

We also reviewed the Agency's work and status in areas highlighted by a President's Council on Integrity and Efficiency report, *Key Escrow Management and File Encryption Challenges for the Federal Inspector General Community*, issued in June 2008. The report addressed concerns related to protection of Personally Identifiable Information (PII), OIG access to records, and key escrow management.[2] While these issues are not

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

[2] Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow by a third party so that, under certain circumstances, an authorized third party may gain access to those keys.

expressly discussed in the OMB's FY 2008 FISMA guidance, they are closely related to the intent of FISMA and OMB's emphasis on the protection of PII. Therefore, we have included steps to address these issues in our review.

We performed field work at SSA facilities nationwide from March to September 2008. We considered the results of other OIG audits performed in FY 2008. 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.

Systems Certified and Accredited in Fiscal Year 2008

#	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	EWAN
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	Lenel Security Access System	LSAS
11	Quality Assurance Systems	QA
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	Recovery of Overpayments, Accounting and Reporting System	ROAR
4	Retirement, Survivors & Disability Insurance Accounting System	RSDI
5	Social Security Number Enumeration and Correction System	SSNECS
6	Supplemental Security Income Record Maintenance System	SSIRMS
7	Title II System	T2

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Information Technology Audit Division, (410) 965-9702

Phil Rogofsky, Audit Manager, Information Technology Audit Division, (410) 965-9719

Acknowledgments

In addition to the persons named above:

Grace Chi, Auditor in Charge

Tina Nevels, Auditor

Michael Zimmerman, Auditor

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 Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-08-18063.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget

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.