FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2007 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act

September 2007 **A-14-07-17101**

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 24, 2007 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2007 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-07-17101)

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) 2007.[1]

BACKGROUND

FISMA provides the framework for securing the Federal Government's 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 each agency to develop, document and implement an agencywide information security program.[2]

OMB uses information reported pursuant to FISMA to evaluate agency-specific and governmentwide security performance, develop the annual security report to Congress, and assist in improving and maintaining adequate agency security performance. OMB issued FY 2007 FISMA guidance (FISMA guidance) on July 25, 2007.[3] This guidance references and incorporates the requirements[4] of OMB Memoranda M-06-15[5] and M-06-19.[6] For additional information, see Appendix C.

---

[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).

[3] OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 25, 2007.

[4] OMB M-07-19 supra at pages 33-34.

[5] OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006.

[6] 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.

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.[7] SSA's OIG contracted with PricewaterhouseCoopers, LLP (PwC) to audit SSA's FY 2007 financial statements.[8] Because of the extensive internal control system review work 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 performed an "agreed-upon procedures" engagement using FISMA, OMB, the 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.[9] See Appendix D for more details on our Scope and Methodology.

SUMMARY OF RESULTS

Based on the results of the OIG's and PwC's audit work, we determined that SSA substantially met the FISMA requirements for FY 2007. SSA continues to work towards maintaining a secure environment for its information and systems and has made improvements over the past year to further strengthen its compliance with FISMA. For example, SSA continues to have sound remediation, certification and accreditation, and inventory processes. In FY 2007, SSA completed an inventory of all systems and subsystems. The SSA systems inventory consisted of 20 major systems as well as over 300 subsystems. Our review found the FY 2007 inventory is accurate and complete.

SSA also maintained Certifications and Accreditations (C&A) for all 20 major systems and conducted recertifications of 12 major systems using NIST Special Publication 800-37 guidance.[10] We reviewed all 20 C&As for the major systems and they were substantially compliant with NIST 800-37. See Appendix E for the complete list of major systems that were certified and accredited in FY 2007.

---

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

[8] OIG Contract Number GS-23F-0165N, dated March 16, 2001. FY 2007 option was exercised on November 30, 2006.

[9] OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 25, 2007.

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

We noted several areas that would enhance security of SSA's systems and sensitive information. SSA should ensure:

- controls to protect personally identifiable information (PII) are fully developed and implemented in accordance with OMB guidance;
- adequate incident response and reporting policies and procedures are implemented agencywide;
- system access controls are fully implemented to meet least privilege criteria for all users of SSA's systems;
- all contractor personnel receive annual security awareness;
- all employees and contractor personnel with significant IT security responsibilities should receive specialized training; and
- the Privacy Impact Assessment (PIA) process appropriately addresses privacy and PII protection issues.

SSA'S EFFORTS TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION

In May 2007, OMB issued Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,*[11] to further address Government efforts to protect PII. The FISMA guidance[12] requires agencies to include the following plans required by M-07-16 as an appendix to their annual FISMA report:

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

SSA has taken numerous steps to address OMB guidance on PII. In September 2006, the Agency released, *Policy and Procedures for All SSA Employees for Reporting the Loss or Suspected Loss of Personally Identifiable Information*.[13] This policy requires the reporting of incidents involving the loss or potential loss of PII within 1 hour of discovery. In March 2007, the Agency issued procedures on safeguarding PII while in transit or outside of secure SSA space. In August 2007, SSA issued the Agency's Draft *SSA Breach Notification Policy* for comments. SSA is also working to eliminate

[11] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* May 22, 2007.

[12] OMB M-07-19, supra at cover page.

[13] Information Systems Security Handbook (ISSH), Appendix V, http://eis.ba.ssa.gov/ssasso/incidentrptg.htm.

unnecessary use of the SSN and to reduce holdings of PII. The Agency has a policy outlining rules of behavior,[14] but needs to improve Agencywide procedures to ensure better identification of violations and corrective actions. Stronger procedures will likely result in more consistent and appropriate handling of violations and improve the effectiveness of the rules of behavior as a deterrent for inappropriate activity.

The Agency has also established workgroups, a PII Executive Steering Committee, 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 a breach occurs. SSA has not included the OIG in its data breach core management group as recommended by OMB.[15] By including the OIG in this group, SSA will be better able to respond to data losses and fully comply with OMB requirements.

While developing its plan to reduce unnecessary use of SSNs, as required by OMB,[16] SSA should take into consideration 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 that contractors are only receiving information that they need to know. Additionally, SSA should also review information contained in the Death Master File and determine what happens when individuals are erroneously reported as deceased. SSA should 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 such as those identifying consequences and corrective actions available for failure to follow the rules of behavior.

IMPLEMENTATION OF INCIDENT RESPONSE POLICIES AND PROCEDURES

FISMA requires Federal agencies to develop, document, and implement an agencywide information security program that includes procedures for detecting, reporting, and responding to security incidents.[17] SSA follows documented policies and procedures for reporting cyber and physical incidents internally. The Agency's ISSH *Security Incident Identification, Reporting, and Resolution*, contains the documented cyber incident

[14] ISSH, *Rules of Behavior for Users and Managers of SSA's Automated Information Resources,* March 23, 2001.

[15] OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification,* September 20, 2006, page 2.

[16] OMB M-07-16, supra at page 7.

[17] 44 U.S.C. § 3544(b) and (b)(7).

reporting policies and procedures.[18] For the physical incidents, SSA's Automated Information Management System contains internal reporting policies and procedures for physical security incidents.[19]

SSA also has documented policies and procedures for reporting physical and cyber incidents to law enforcement authorities. SSA's Intrusion Protection Team has policies and procedures for reporting incidents to law enforcement authorities. These policies and procedures meet FISMA requirements by having the Agency send appropriate cases to SSA's OIG. However we observed in our Incident Response and Reporting review,[20] that the Agency did not consistently notify OIG's Office of Investigations (OI) when security incidents occurred. The OI could have assisted in the preservation of electronic evidence and potentially pursued issues for further investigation. The Agency subsequently informed us that its components will do their utmost to provide all incidents to OI. We look forward to this revised procedure and will work with the Agency to ensure that all incidents are forwarded to OI. OI's Electronic Crimes Team also has policies and procedures for reporting cyber incidents to other law enforcement authorities, if necessary. The Agency has policies and procedures contained in the ISSH for reporting physical incidents to law enforcement.

SSA has documented policies and procedures for reporting internally and to law enforcement. However, the Agency needs to clarify and fully implement its written procedures for reporting security incidents to US-CERT. As noted in our Incident Response and Reporting review,[21] SSA also needs to properly categorize and report computer-related security incidents in accordance with NIST and US-CERT criteria. US-CERT coordinates information received from all Federal agencies to defend the Federal Government against and respond to cyber attacks. By providing US-CERT with all appropriate information, US-CERT's efforts to protect the Federal Government will be enhanced. The Agency needs to ensure that the formal written procedures are fully disseminated and implemented consistently with its policy so all appropriate incidents are provided to US-CERT.

---

[18] ISSH, Chapter 7, *Security Incident Identification, Reporting and Resolution*, November 15, 2006.

[19] Administrative Instructions Manual System, General Administration Manual, Chapter 12, Instruction Number 07, *Incident Alert Reporting*, June 19, 2006.

[20] OIG Report, *The Social Security Administration's Incident Response and Reporting System* (A-14-07-17070), pp. 9, 10, August 3, 2007.

[21] OIG Report A-14-07-17070, supra at p.4.

IMPLEMENTATION OF SYSTEM ACCESS CONTROLS

Controlling and limiting systems access to the Agency's information systems and resources is the first line of defense in assuring 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 auditor's financial statement report. However, we noted instances where SSA's access controls could be strengthened. One area involved access to sensitive data held by DDS employees.[22] These are State employees who perform services for SSA and periodically need to access SSA records.

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 has never been changed; and
- the need for access to each resource contained in the DDS profiles had not been documented for DDS employees.

Another area that could be strengthened involved employment suitability checks of SSA contractor personnel. We found that a number of the contractor staff involved in office relocations did not receive background checks.[23] Therefore, they should not have been permitted to work on-site at an SSA facility or have physical access to Agency hardware that may have contained programmatic or sensitive information. As a result, SSA maybe 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

Identifying Individuals with Significant IT Security Responsibilities

According to OMB FISMA guidance, agencies are required to ensure that employees and contractor personnel with significant IT security responsibilities receive security awareness and specialized training.[24] SSA ensures that security awareness is provided to all employees by requiring them to annually read the *Sanctions for Unauthorized*

[22] OIG Formal Draft, *Access to SSA Data Provided by Disability Determination Services Positional Profiles* (A-14-07-17024), August 23, 2007.

[23] OIG Report, *The Social Security Administration's Information Technology Maintenance and Local Area Network Relocation Contract* (A-14-07-17022), pp. 3-4, May 21, 2007.

[24] OMB M-07-19, supra at page 18

Systems Access Violations and sign that they have read and understand this document.[25] However, we noted areas that need improvement.

SSA needs to improve its identification of all individuals, both employees and contractors, with significant IT security responsibilities. Currently, the Agency has developed and implemented the following definition for the employees with significant IT security responsibilities:

> 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.[26]

SSA's practice is that each component uses this definition to determine which of its employees have "… significant IT security responsibilities." The Agency reviewed individuals' responsibilities to comply with FISMA. SSA seems to be defining people with significant security responsibility as those who spend a significant portion of their work time on IT security issues. Individuals responsible for physical controls over Agency IT resources or those who have the ability to significantly impact security controls should be designated as having significant IT responsibilities.

For example, it would benefit SSA to include the individuals who oversee the e-mail system as those with significant security responsibilities. E-mail continues to be a major source of vulnerability throughout the cyber world. Lack of adequate controls of an organization's e-mail system could lead to major network and system problems. SSA can reduce its risks by refining its classification of individuals with significant IT security responsibilities and ensuring that these individuals receive adequate training.

Additionally, the Agency did not consider any of its 22,098 contractors to have significant IT security responsibility because every decision made or action taken was approved or carried out by Agency personnel. Although the Agency may not consider these contractors to have significant IT security responsibilities, there are numerous contractors that work in the areas of firewall protection, intrusion protection, physical and systems security that should be considered as meeting the definition of individuals with significant IT security responsibilities.

---

[25] SSA Office of Labor Management and Employee Relations, *Sanctions for Unauthorized System Access Violations,* page 1, June 1998.

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

Security Awareness for Contractors

SSA needs to improve monitoring of security awareness notifications received by the Agency's contractors. SSA has a policy requiring all contractor personnel to read and sign the annual security awareness statement. SSA staff indicated that all contractor personnel are provided the same security awareness notifications as its employees. However, because the Agency did not centrally maintain and monitor the security awareness efforts for its contractors, SSA could not provide supporting documentation to substantiate that the Agency complied with the requirement for security awareness for contractors. SSA plans to change its monitoring process to improve tracking of contractor security awareness.

It should be noted that OMB's FISMA guidance asked for OIGs and agencies to report on security awareness training in slightly different manners. Agencies were only asked an overall "Yes/No" question as to whether all employees and contractors were provided security awareness.[27] OIGs were asked the percentage of the combined employees and contractors who received security awareness.[28] According to OMB FISMA guidance, all employees, regardless whether they have systems access, should receive annual security and privacy awareness training.[29] Contractors must be trained on agency-specific security policies and procedures, including rules of behavior.[30] By not monitoring contractor training and awareness, contractors may access SSA's systems without being fully aware of or appropriately trained in how to handle SSA's sensitive information. SSA needs to ensure appropriate security awareness and training is provided to contractor personnel. As system owners, SSA has the ultimate responsibility to ensure those who could impact its systems have sufficient security awareness and training.

[27] OMB M-07-19, supra at page 26.

[28] OMB M-07-19, supra at pages 34-35.

[29] OMB M-07-19, supra at page 18.

[30] Id.

PERFORMANCE OF THE PRIVACY IMPACT ASSESSMENTS

The E-Government Act[31] and OMB M-03-22[32] require agencies to perform PIAs for systems that collected PII from the public in certain situations.[33] A PIA is defined as

> …an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[34]

Sixteen of SSA's 20 significant systems collect PII from the public. During our fieldwork, SSA provided 2 dedicated and 9 associated PIAs for these 16 systems. The PIAs reviewed followed the procedures documented in '*PIA info from PRIDE.*'[35] Based on the results of our review, we determined and SSA agreed that dedicated PIAs were needed for the remaining 14 systems. On September 4, 2007, SSA provided the OIG with the dedicated draft PIAs for the 14 remaining systems, which appeared to be prepared properly. SSA plans to finalize the dedicated PIAs for the remaining 14 systems by September 30, 2007. SSA needs to follow through with its plan to finalize these 14 draft PIAs by end of September. In the future, completing the appropriate PIAs in a timely manner will enable SSA to better address the risks involved with the collection and protection of sensitive information.[36]

CONCLUSIONS AND RECOMMENDATIONS

During our FY 2007 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.

---

[31] E-Government Act of 2002, Pub. L. No. 107-347 § 208B.1.a., December 17, 2002.

[32] OMB Memorandum, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, pages 3 and 8, September 26, 2003.

[33] The E-Government Act of 2002, supra, requires an agency to conduct a PIA before developing or procuring certain information technology, or initiating certain new collections of information in identifiable form that will use information technology.

[34] OMB Memorandum, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A § II.A.6., September 26, 2003.

[35] PRIDE is SSA's rules and guidelines for developing new systems and applications.

[36] E-Government Act of 2002, supra, § 208B.1, OMB Memorandum, M-03-22, supra.

To fully comply and ensure future compliance with FISMA and other information security related laws and regulations, we recommend SSA ensure:

1. controls to protect PII are fully developed and implemented in accordance with OMB guidance;

2. adequate incident response and reporting policies and procedures are implemented Agencywide;

3. system access controls are fully implemented to meet least privilege criteria for all users of SSA's systems;

4. refinement efforts continue for its categorization of Agency and contractor personnel with significant IT security responsibility and ensure that appropriate training is provided;

5. all contractor personnel receive annual security awareness; and

6. the PIA process is completed timely and that it appropriately addresses privacy and PII protection issues.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

C&A	Certifications and Accreditations
DDS	Disability Determination Services
FIPS	Federal Information Processing Standard
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
ISSH	Information Systems Security Handbook
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OI	Office of Investigations
OMB	Office of Management and Budget
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
Pub. L.	Public Law
POA&M	Plan of Action and Milestones
PwC	PricewaterhouseCoopers LLP
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 OMB Questions Concerning 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: 9/24/07**

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	
Social Security Administration	**FIPS 199 System Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
	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
Agency Totals	**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							
		a. Number of systems certified and accredited		**b. Number of systems for which security controls have been tested and evaluated in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
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		
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 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 systems that are missing from the inventory. Missing Agency Systems Missing Contractor Systems	N/A

Question 4		
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 agencywide 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).	- Almost Always, for example, approximately 96-100% of the time
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% 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: 4a & 4c. Agency should continue to monitor the process to ensure that all findings are included in the process.		

Question 5

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	- Excellent

5.b.	The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	

C&A process comments:

Question 6		
6.a.	Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards. Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments: Sixteen of SSA's twenty significant systems collect PII from the public. During our fieldwork, SSA provided 2 dedicated and 9 associated PIAs of these 16 systems. The Agency follows the procedures in the document entitled *"PIA info from PRIDE"*[1] to determine whether a PIA is required. Based on the results of our review, we determined and SSA agreed that dedicated PIAs were needed for the remaining 14 systems. On September 4, 2007, SSA provided the OIG with the dedicated draft PIAs for the 14 systems that collect public PIA, which appear to be completed appropriately. SSA plans to finalize the dedicated PIAs for the remaining 14 systems by September 30, 2007. Completing the appropriate PIAs will enable SSA to better address the risk involved with the collection and protection of sensitive information.		
6.b.	Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII). Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Good
Comments: SSA has taken considerable steps to safeguard PII. They have established a policy to report incidents involving the loss or potential loss of PII to US-CERT. They have issued procedures on safeguarding PII while in transit or outside of secure SSA space. They are developing a *SSA Breach Notification Policy* scheduled for issuance September 30, 2007. SSA still needs to finalize and fully implement these new policies and procedures. Due to the time frame, the OIG has not yet had the opportunity to test the effectiveness of all the controls recently issued.		

[1] PRIDE is SSA's rules and guidelines for developing new systems and applications.

Question 7		
7.a.	Is there an agency-wide security configuration policy? Yes or No.	Yes
Comments:		
7.b.	Approximate the extent to which applicable information systems apply common security configurations established by NIST. 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
Comments:		

Question 8		
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.		
8.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
8.b.	The agency follows documented policies and procedures for external reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov. Yes or No.	Yes
8.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments: 8b. SSA needs to ensure that the policies and procedures are fully disseminated to the appropriate staff and fully implemented. 8c. The Agency informed us that its components will do their utmost to provide all incidents to OI. We look forward to this revised procedure and will work with the Agency to ensure that all incidents are forwarded to OI.		

Question 9	
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: All 64,170 SSA employees have received annual security awareness. SSA has a policy for all contractors to receive security awareness annually, but could not confirm that the policy was adhered to. Therefore, we could only confirm that 64,170 employees the 86,268 employees and contractors, or 74%, have received security awareness. Next year, SSA plans to establish a contractor monitoring process for security awareness.	
Question 10	
Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agencywide training? Yes or No.	Yes
Question 11	
The agency has completed system e-authentication risk assessments. Yes or No.	Yes

Background and Current Security Status

The Federal Information Security Management Act (FISMA) requires agencies to 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 2005, Social Security Administration (SSA) resolved the long standing internal controls reportable condition concerning its protection of information.[2] SSA continues to work with the Office of the Inspector General and PricewaterhouseCoopers LLP to further 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 M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. This new guidance mandates agencies increasing efforts to reduce the use of PII collected and held. OMB M-07-16 complements existing PII guidance contained in OMB Memorandum M-06-15 and OMB Memorandum M-06-19. OMB is incorporating more privacy and PII protection questions in its annual FISMA guidance. OMB M-07-19 requires agencies to include in their annual FISMA submission:

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

In addition, OMB guidance M-07-19 requires Inspectors General to rate the quality of Agencies' Privacy Impact Assessment process and their efforts to protect PII according to OMB M-06-15.

[1] Pub. L. 107-347, Title III, Section 301, 44 U.S.C. § 3544.

[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 governmentwide IT security strengths and weaknesses and a plan of action to improve performance. It also examines agency status against key security and privacy performance measures from Fiscal Year (FY) 2002 through FY 2006. 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) 2007 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-07-19, *FY 2007 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 2007 *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 2007 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), 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.

We performed field work at SSA facilities nationwide from March to September 2007. We considered the results of other OIG audits performed in FY 2007. Our evaluation was performed in accordance with generally accepted government auditing standards.

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

Systems Certified and Accredited in Fiscal Year 2007

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

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

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

Acknowledgments

In addition to the persons named above:

Mary Ellen Moyer, Senior Program Analyst

Deborah Kinsey, Senior 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 Specialist at (410) 965-3218. Refer to Common Identification Number A-14-07-17101.

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 our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

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

Office of Investigations

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

Office of the Chief Counsel to the Inspector General

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

Office of Resource Management

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