FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2006 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act

September 2006   A-14-06-16084

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

Mission

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

Authority

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

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

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

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

Vision

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

SOCIAL SECURITY

MEMORANDUM

Date: September 22, 2006 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2006 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-06-16084)

OBJECTIVE

Our objective was to determine if 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) 2006.[1]

BACKGROUND

FISMA provides the framework for securing the Federal Government's information technology. 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.

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 2006 FISMA guidance on July 17, 2006.[2] This guidance references and incorporates the requirements of OMB Memoranda M-06-15[3] and M-06-19.[4] For additional information, see Appendix C.

[1] Public Law 107-347, Title III, Section 301.

[2] OMB Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 17, 2006.

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

[4] 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.[5] SSA's OIG contracted with PricewaterhouseCoopers, LLP (PwC) to audit SSA's FY 2006 financial statements.[6] 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.[7] See Appendix D for more details on our Scope and Methodology.

SUMMARY OF RESULTS

During our FY 2006 evaluation, we determined that SSA generally met the FISMA requirements. 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 2006, 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 that the FY 2006 inventory is accurate and complete.

SSA also maintained Certifications and Accreditations (C&A) for all 20 major systems and conducted recertifications of 7 major systems using the NIST Special Publication 800-37 guidance.[8] 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 2006.

[5] Public Law 107-347, Title III, Section 301, 44 U.S.C. § 3545 (b)(1).

[6] OIG Contract Number GS-23F-0165N, dated March 16, 2001. FY 2006 option was exercised on November 10, 2005.

[7] OMB Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* July 17, 2006 and NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

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

We noted several areas that SSA needs to address to fully meet FISMA requirements while enhancing information management in this area. Nothing came to our attention to indicate that these issues would cause SSA to be non-compliant with FISMA. SSA should ensure that:

- system access controls are adequately reviewed using a risk-based approach on a consistent basis across the Agency;

- all Information Technology (IT) security weaknesses that are identified are reported to the Office of the Chief Information Officer (OCIO) and are subject for inclusion in Automated Security Self-Evaluation and Remediation Tracking (ASSERT);

- complete, current and accurate information systems security policies and procedures are maintained and are accessible to appropriate employees;

- all agency and contractor personnel with significant IT security responsibilities are identified and receive annual security awareness training; and

- the Continuity of Operations Plan (COOP) and Disaster Recovery Exercise (DRE) are updated and tested appropriately.

Based on the OMB FISMA guidance,[9] the SSA is supposed to provide additional information on its response to OMB M-06-15 and M-06-19. OMB memorandum M-06-15 re-emphasizes the protection of Personally Identifiable Information and requires that the agency Senior Official for Privacy conduct a review. The SSA Senior Official for Privacy conducted the required review and issued a report. Also, OMB Memorandum M-06-19 requires agencies to report all incidents involving Personally Identifiable Information to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour of discovery. Based on our discussions with the Agency, SSA is currently redefining its interpretation of what an incident is to ensure full compliance with OMB M-06-19. Subsequent to the issuance of M-06-19, SSA has reported several incidents to US-CERT.

While the OIGs do not have reporting requirements in these areas, we did review the SSA Senior Official for Privacy's report and nothing came to our attention that led us to believe that there were any significant omissions from this process. Further, since the Agency is still drafting its response to OMB M-06-19, we were unable to complete any work in this area.

[9] OMB M-06-20, supra at cover page.

ENSURE SYSTEM ACCESS CONTROLS ARE ADEQUATELY REVIEWED

NIST Special Publication 800-53a[10] requires that agencies have formal documented access control policies and procedures that are reviewed and updated on a regular basis. These reviews should be risk-based and consistently applied across the Agencies. SSA has established a control that grants access to IT resources based on a user profile.[11] A user profile is created based on each individual job's responsibilities. SSA completed a review of user profiles across the Agency during the reporting period. However, we found SSA did not have clear policies and procedures on how the review should be conducted. As a result, instances of excessive access were not identified and corrected by the Agency and users continued to have excessive access. SSA should ensure that user profiles only provide access to systems resources necessary to meet user job requirements. SSA needs to strengthen its access control processes to ensure that the user profiles are adequately reviewed and tested.

ENSURE THAT ALL IDENTIFIED IT SECURITY WEAKNESSES ARE INCLUDED IN THE AGENCY'S REMEDIATION PROCESS

OMB FISMA guidance states that all IT system security weaknesses be reported and tracked through remediation in one central location.[12] The OCIO was designated by SSA as the responsible component. The SSA OCIO, using the software tool ASSERT, established a system to monitor and report on IT security weaknesses. ASSERT is also used to support the Plan of Action & Milestones (POA&M) process that tracks identified IT security weaknesses through remediation.

While we found that the SSA OCIO ASSERT tool was working effectively, we also learned that the OCIO did not receive all reports on IT security weaknesses. We identified reviews that were conducted by an SSA contractor during the current reporting cycle that focused on assets that are critical to the SSA IT infrastructure. These reviews identified multiple IT security weaknesses that need to be recognized, included and addressed as part of the ASSERT process.

The Agency is in the process of developing policies and procedures to ensure that all IT security weaknesses are appropriately included in the tracking and remediation process. The Agency needs to ensure that these policies and procedures are adhered to and fully implemented.

[10] NIST Special Publications 800-53a, Guide for Assessing the Security Controls in Federal Information Systems, April 2006, page 42.

[11] User profiles provide a means to classify groups of individuals who share common access needs for similar job requirements. Top Secret security software controls the user profiles, as well as monitors who can access and change critical data requirements.

[12] OMB M-06-20, supra at page 7.

INFORMATION SYSTEMS SECURITY POLICIES AND PROCEDURES NEED TO BE CURRENT, COMPLETE, AND AVAILABLE TO AGENCY PERSONNEL

Adequate security policies and procedures that are used throughout the Agency are essential to ensure an effective management oversight process as well as a sound security framework required by FISMA. SSA's information systems security policy and procedures are driven by the Information Systems Security Handbook (ISSH). The ISSH is accessible on the Agency's Intranet site. During the current reporting period, the Agency was in the process of revising the ISSH and related procedures. At the completion of our fieldwork, the ISSH and related procedures had not been completely revised and updated. The Agency must ensure that a complete, accurate, and current version of Agency security policies and procedures are available to appropriate personnel.

ALL SSA EMPLOYEES AND CONTRACTOR PERSONNEL WHO HAVE SIGNIFICANT IT SECURITY RESPONSIBILITIES NEED TO RECEIVE APPROPRIATE TRAINING

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.[13] SSA ensures that security awareness training is provided to all employees by requiring them to annually read the *Sanctions for Unauthorized Systems Access Violations* and sign that they have read and understand this document.[14] Contractor personal are provided security awareness training by their employer. According to SSA, Agency employees and contractor personnel with specialized security responsibilities are to be provided additional security training.

At this time, SSA has not adopted a policy that clearly defines employees who have "significant IT security responsibilities." SSA's current practice is that each component makes its own interpretation of what constitutes employees who have "significant IT security responsibilities." Based on what the components have determined for the current reporting period, SSA has identified 442 employees with significant IT security responsibilities, of which, 92 percent have completed the required training. Additionally, by not having an Agency-wide policy, it is possible for two employees with the same job responsibilities to be classified differently. Therefore, one individual may receive the appropriate training and the other may not.

Industry and other Federal Government Agencies have a more stringent interpretation of OMB guidance. They have identified many more individuals as meeting the definition of what constitutes an individual with "significant IT security responsibilities."

[13] OMB M-06-20, supra at page 35.

[14] http://eis.ba.ssa.gov/olmer/Links/sanctions/Instructions.htm as of September 15, 2006.

Particularly in light of the additional focus on the security of Personally Identifiable Information, SSA should consider redefining its definition of individuals with “significant IT security responsibilities” to ensure appropriate security training coverage.

SSA CONTINUITY OF OPERATIONS TESTING

FISMA codifies a longstanding policy requirement that each agency’s security program and security plan include provisions in its COOP for information systems that support the operations and assets of the agency.[15] SSA needs to make certain that both the COOP and DRE are updated annually to ensure that the Agency can adequately function in the event of an emergency or disaster. The Agency Intranet and Internet are an integral part of Agency operations, and are currently not included in the COOP or DRE. Agency components have an expectation that these services will be quickly recovered in the event of an interruption or disaster. DRE testing of all critical applications would provide assurance as to the Agency’s ability to recover. The Agency should include applications, such as Internet, Intranet, email and other important systems in the COOP and DRE. Also, the Agency should ensure that the COOP and DRE are updated and tested at least annually.[16]

CONCLUSIONS AND RECOMMENDATIONS

During our FY 2006 FISMA evaluation, we determined that SSA generally met the requirements of FISMA. SSA worked cooperatively with the OIG to identify ways to comply with FISMA. SSA developed and implemented a wide range of security policies, plans, and practices to safeguard its systems, operations, and assets. To fully comply and ensure future compliance with FISMA and other information security related laws and regulations, we recommend SSA ensure:

1. system access controls are adequately reviewed using a risk-based approach on a consistent basis across the Agency;

2. all IT security weaknesses identified are reported to the OCIO and, where appropriate included in ASSERT;

[15] Public Law 107-347, Title III, Section 301, 44 U.S.C § 3544(b)(8).

[16] Federal Emergency Management Agency Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations,* June 15, 2004.

3. complete, accurate and current information systems security policies and procedures are maintained and accessible to appropriate employees;

4. it has developed an appropriate definition of employees and contractors with “significant IT security responsibilities,” and using that definition, has identified and ensured that all such individuals received the necessary security training; and

5. the COOP and DRE include all essential applications and are updated and tested appropriately.

Patrick P. O’Carroll, Jr.

Appendices

Appendix A

Acronyms

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
C&A	Certification and Accreditation
COOP	Continuity of Operations Plan
DRE	Disaster Recovery Exercise
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISCAM	Federal Information System Controls Audit Manual
FY	Fiscal Year
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
PMA	President’s Management Agenda
POA&M	Plan of Action and Milestones
PwC	PricewaterhouseCoopers LLP
SSA	Social Security Administration
US-CERT	United States Computer Emergency Readiness Team

Appendix B

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

Agency Name: Social Security Administration

Question 1

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53.
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. FY 06 Agency Systems		**b. FY 06 Contractor Systems**		**c. FY 06 Total Number of Systems**	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Social Security Administration	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
	Sub-total	**20**	**20**	**0**	**0**	**20**	**20**
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 each part of this question, identify actual performance in FY 06 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

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**	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Social Security Administration	High	0	0.0%	0	0.0%	0	0.0%
	Moderate	8	100.0%	8	100.0%	8	100.0%
	Low	12	100.0%	12	100.0%	12	100.0%
	Not Categorized	0	0.0%	0	0.0%	0	0.0%
	Sub-total	**20**	**100.0%**	**20**	**100.0%**	**20**	**100.0%**
Agency Totals	**High**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	Moderate	**8**	**100.0%**	**8**	**100.0%**	**8**	**100.0%**
	Low	**12**	**100.0%**	**12**	**100.0%**	**12**	**100.0%**
	Not Categorized	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
	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. Self-reporting of NIST Special Publication 800-26 and / or 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. 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
3.b.1	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.b.2	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	None missing
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.	The agency has completed system e-authentication risk assessments.	Yes

Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

- 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.	- Mostly, for example, approximately 81-95% 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, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Mostly, for example, approximately 81-95% of the time
4.d.	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

Comments: 4a & 4c. We have concerns as to whether the OCIO is receiving all IT security weaknesses identified by internal reports on a regular basis.

Question 5	
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. 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 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .	
Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Excellent
Comments:	

Question 6		
6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
Comments:		

6.b.	Configuration guides are available for the products listed below. With a checkmark, identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agency wide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Solaris	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
HP-UX	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Linux	N/A	No	Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software
Other: IBM AS/400 (AIX), IBM zOS	Yes	Yes	Almost Always, or on approximately 96-100% of the systems running this software

Comments: According to SSA, Linux has been removed from all SSA computers connected to the network as of March 29, 2006.

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: 7.c- We still have not received information on how SSA plans to respond to OMB M-06-19.

Question 8

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training

Comments: We have concerns because the number of individuals with significant IT security responsibilities went from approximately 900 reported last year to 452 reported this year. It appears that all of the individuals with significant IT security responsibilities may not have been included in the documentation we received. We are also concerned that we were only provided information on security awareness and training for NCC based contractors.

Question 9

9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? 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, 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.

OMB Memorandum M-06-15[3] reemphasizes existing requirements under the Privacy Act,[4] including the establishment of employee rules of conduct, administrative, technical, and physical safeguards for the protection of Personally Identifiable Information. M-06-15 also requires that the agency's designated Senior Official for Privacy conduct a review of policies and processes, and take corrective action as appropriate to ensure that the agencies have adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, Personally Identifiable Information.[5] This review is required to address all administrative, technical, and physical means used by SSA to control such information, including but not limited to procedures and restrictions on the use or removal of Personally Identifiable Information beyond Agency premises or control.[6] This review is also required to be completed by SSA in time for inclusion in the annual FISMA report. In addition, any weaknesses identified in Agency security plans of action and milestones are required to be reported. Also, employees are to be reminded within 30 days of the issuance of M-06-15 of their specific responsibilities for safeguarding Personally Identifiable Information, the rules for acquiring and using such information as well as the penalties for violating these rules.

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

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

[3] OMB M-06-15, supra at page 1.

[4] 5 U.S.C. § 552a(e)(9)-(10).

[5] OMB M-06-15, supra.

[6] OMB M-06-15, supra at page 1-2.

OMB Memorandum M-06-19[7] provides updated guidance in two areas. The first area addresses the reporting of security incidents involving Personally Identifiable Information. The new reporting procedures now require agencies to report all incidents involving Personally Identifiable Information to US-CERT within 1 hour of discovery either in electronic or physical form and agencies are not to distinguish between suspected and confirmed breaches. The second area addressed by M-06-19 reminds departments and agencies that security and privacy requirements should be included in fiscal year budget submissions for IT. Additional detail is also requested on how resources will be allocated in correcting existing security weaknesses.

[7] OMB M-06-19, supra.

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 (SSA) OIG contracted with PricewaterhouseCoopers LLP (PwC) to audit SSA's Fiscal Year (FY) 2006 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-06-20, *FY 2006 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 Memoranda M-06-15 and M-06-19. We reviewed SSA's Senior Official for Privacy report for 2006, monitored US-CERT reporting activity, and SSA's response to M-06-19.

The results of our FISMA evaluation are based on the PwC FY 2006 *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 2006 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 all 20 C&As for each major system. 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 2006. Our evaluation was performed in accordance with generally accepted government auditing standards.

[1] Public Law 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 2006

#	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	Disability Control File System	DCFS
7	Enterprise Wide Area Network and Services System	EWANSS
8	FALCON Data Entry System	FALCON
9	Human Resources Management Information System	HRMIS
10	Integrated Client Database	ICDB
11	Logiplex Security Access Systems	LSAS
12	Recovery of Overpayments, Accounting, & Reporting System	ROAR
13	Social Security Online Accounting and Reporting System	SSOARS
14	Social 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 Records Maintenance System	SSIRMS
6	Title II System	

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:

Harold Hunter, Senior Auditor

Annette DeRito, Writer/Editor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-14-06-16084.

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.