FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2005 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act

A-14-05-15060

September 2005 **Patrick P. O'Carroll, Jr. – Inspector General**

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

MEMORANDUM

Date: September 16, 2005 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2005 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-05-15060)

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).[1]

BACKGROUND

FISMA provides the framework for securing the Federal Government's information technology including both unclassified and national security systems. 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 the information to help evaluate agency-specific and government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and inform development of the eGovernment (eGov) Scorecard under the President's Management Agenda (PMA).

OMB developed a traffic light scorecard to show the progress agencies have made: green for success, yellow for mixed results, and red for unsatisfactory. SSA's current status is yellow and its score for progress in implementing eGov services is green. Many of the elements of the eGov initiative overlap or duplicate the requirements of FISMA. In our results of review, we highlight when the FISMA issue also impacts whether the Agency can meet the eGov security requirements. See Appendix C for more background.

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

SCOPE AND METHODOLOGY

FISMA directs each agency's Office of the Inspector General (OIG) to perform an annual, independent evaluation of the agency's information security program and practices.[2] SSA's OIG contracted with PricewaterhouseCoopers, LLP (PwC) to audit SSA's Fiscal Year (FY) 2005 financial statements.[3] 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 reviews of SSA's mission critical sensitive systems as described in the Government Accountability Office's *Federal Information System Controls Audit Manual*. PwC performed an "agreed-upon procedures" engagement using FISMA, OMB and the National Institute of Standards and Technology (NIST) guidance, 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.[4] See Appendix D for more details on our Scope and Methodology.

SUMMARY OF RESULTS

During our FY 2005 FISMA evaluation, we determined that SSA has generally met the requirements of FISMA. 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. Among the elements of its secure environment are sound remediation, certification and accreditation, and inventory processes. To fully meet the requirements of FISMA and enhance information management in this area, SSA should:

- Fully comply with the Agency's risk models and configuration guides;
- Ensure that the Continuity of Operations Plan (COOP) is updated and tested appropriately;
- Improve monitoring of contractor security awareness training; and
- Formalize the policy and procedures for maintaining the systems inventory.

SSA'S REMEDIATION, CERTIFICATION AND ACCREDITATION, AND INVENTORY PROCESSES ARE PERFORMING ADEQUATELY

During FY 2004, SSA implemented a software tool, Automated Security Self-Evaluation and Remediation Tracking (ASSERT), to monitor and report system security weaknesses. ASSERT also tracks the remediation process for those weaknesses. SSA continues to effectively monitor its remediation process through the use of the

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

[3] OIG Contract Number GS-23F-0165N, dated March 16, 2001. FY 2005 option was exercised on November 29, 2004.

[4] OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* June 13, 2005 and NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

ASSERT software tool in accordance with FISMA and OMB FISMA guidance.[5] Currently, ASSERT properly tracks over 50 security weaknesses. None of the weaknesses tracked in ASSERT were reported to OMB in SSA's second and third quarter reports during FY 2005. Although the Agency has a Financial Statement reportable condition[6] to improve its protection of information, the Agency chose to only report weaknesses for January through June 2005 to OMB based on the OMB FISMA guidance definition of significant deficiency.[7] OIG works with the Office of the Chief Information Officer to ensure that the ASSERT database is complete and corrective actions are undertaken to remediate the security weaknesses.

SSA, in FY 2004, completed an inventory of all systems and subsystems consisting of 20 major systems as well as over 300 subsystems. SSA updated the systems inventory in FY 2005 and based on our review, it appears to be complete. As of September 2005, SSA did not have a policy to update its systems inventory. Such a policy is needed to effectively update and maintain the systems inventory. The Agency is in the process of developing this policy.

SSA prepared Certifications and Accreditations (C&A) for each of the 20 major systems in accordance with NIST Special Publication 800-37. We reviewed the 20 C&As for the major systems. During the course of our audit, we did note several outdated items in one of the C&As. These items were brought to the Agency's attention and immediately corrected. Nothing came to our attention that led us to believe that there were any significant omissions from the C&A process. As a result, over 90 percent of the Agency's major systems and subsystems were covered by the C&As. See Appendix E for the complete list of major systems that were certified and accredited in FY 2005.

The successful implementation of these security measures has helped SSA maintain a sound security program that complies with FISMA.

SYSTEMS NEED TO FULLY COMPLY WITH SECURITY CONFIGURATIONS

OMB FISMA guidance and the PMA management scorecard requires agencies to develop configuration standards for their Information Technology (IT) systems and have the systems installed and maintained in accordance with these security configuration standards.[8] SSA developed risk models for all operating systems used in its networks.

[5] Public Law 107-347, Title III, section 301, 44 U.S.C. §3544 (b)(6) and OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* June 13, 2005.

[6] SSA's FY 2004 *Performance and Accountability Report,* page 212.

[7] OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, (page 8) states that a significant deficiency under FISMA is comparable to a material weakness under the Federal Managers Financial Integrity Act.

[8] OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* June 13, 2005, pages 15-17 and 23-25 and PMA scorecard standards at *http://www.whitehouse.gov/results/agenda/standards.pdf* as of August 18, 2005, page 4.

In addition, SSA is developing a single configuration guide for all other system components and a separate appendix for various components such as Oracle.

It was observed that the Office of the Actuary had a small number of Linux servers that were connected to the SSA network for most of FY 2005. SSA does not have any risk models for the Linux operating system. SSA has decided to take the Linux servers off the system since they do not have any risk models for Linux. The plan is to have Linux servers removed from the SSA network and out of operation by September 30, 2005. They will be replaced with servers for which SSA has risk models.

To determine compliance with the Agency's risk models, we tested a number of servers for the Unix and Windows 2000 operating systems. The results of our testing disclosed instances of noncompliance with the risk models or configuration guide. Computers that are not in compliance with the Agency risk models are more vulnerable to security threats imposed by hackers, computer viruses, worms, and denial of service attacks. By ensuring that Agency computers are in compliance with their risk models, SSA can better secure the valuable information that has been entrusted to its care.

SSA CONTINUITY OF OPERATIONS TESTING

FISMA codifies a longstanding policy requirement that each agency's security program and security plan include the provision for a COOP for information systems that support the operations and assets of the agency.[9] Additionally, the eGov initiatives require agencies to consolidate and optimize all infrastructures for their COOPs.[10] SSA did participate in the Governmentwide COOP exercise in June 2005. This desk top review included a test of all the major information systems and met the OMB requirement for an annual contingency test.

SSA continues to address its COOP and Disaster Recovery Exercise (DRE) issues for the entire Agency. SSA needs to make certain that both COOP and DRE are updated annually to ensure the Agency can adequately function in the event of an emergency or disaster. Specifically, the Agency should add new applications, such as Internet and Intranet and other important systems to the COOP and DRE. For the past several years, SSA performed an annual week-long DRE in May or June. During the exercises, the major systems were tested to see if they would perform in the event of a disaster. The Agency's last DRE was in June 2004. This year, the Agency postponed its DRE until January or February 2006 because it felt, and we concurred, that it would be better to expand the test into a 2-week exercise. The Agency's DRE contractor was unable to accommodate SSA until 2006.

Furthermore, the COOP did not address information and information systems provided or managed by other agencies, contractors or other sources. For example, SSA relies heavily upon other Federal and State Government agencies such as State Disability Determination Services and the Department of Treasury. In the event of a disaster,

[9] Public Law 107-347, Title III, section 301, 44 U.S.C § 3544(b)(8)).
[10] *http://www.whitehouse.gov/results/agenda/standards.pdf* as of August 18, 2005, page 4.

SSA is uncertain as to the availability of these agencies. SSA should ensure that its COOP is updated and tested appropriately.[11]

SSA NEEDS TO BETTER MONITOR CONTRACTOR SECURITY AWARENESS AND TRAINING

SSA provides security awareness training to all employees and information security training to employees with specialized security responsibilities. SSA modified its systems to more accurately track the IT security training provided to each employee. According to OMB's guidance, agencies are required to ensure that contractors with significant security responsibility have security awareness and specialized training.[12] The Agency has numerous contractors who perform major IT security tasks such as monitoring firewalls. Some of these contractors have received security awareness training and specialized security training, but SSA does not fully monitor or review the security awareness or specialized training of all contractors. All contractors who have access to SSA systems should have an annual security awareness training to ensure that they are knowledgeable of the importance of protecting SSA's sensitive information. Contractors who perform technical IT security functions should receive specialized training on a regular basis. SSA should consider monitoring its contractors better to ensure that they have adequate security awareness and specialized systems training.

CONCLUSION AND RECOMMENDATIONS

During our FY 2005 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:

1. Ensure all computers and servers comply with Agency's risk models and configuration guides;

2. Ensure that the COOP is updated and tested appropriately;

3. Improve monitoring of contractor security awareness training; and

4. Formalize policy and procedures for maintaining the systems inventory.

Patrick P. O'Carroll, Jr.

[11] Federal Emergency Management Agency Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP),* June 15, 2004, pages 1, 4, 8, 9 and I-1.

[12] OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* June 13, 2005, page 15.

Appendices

Appendix A

Acronyms

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
C&A	Certification and Accreditation
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
DRE	Disaster Recovery Exercise
eGov	eGovernment
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
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 05 Agency Systems		**b. FY 05 Contractor Systems**		**c. FY 05 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	7	7	0	0	7	7
	Low	13	13	0	0	13	13
	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	**7**	**7**	**0**	**0**	**7**	**7**
	Low	**13**	**13**	**0**	**0**	**13**	**13**
	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 05 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	7	100.0%	7	100.0%	7	100.0%
	Low	13	100.0%	13	100.0%	13	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	**7**	**100.0%**	**7**	**100.0%**	**7**	**100.0%**
	Low	**13**	**100.0%**	**13**	**100.0%**	**13**	**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 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.	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.	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.	- 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, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% 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:

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. 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 agencywide 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	Mostly, or on approximately 81-95% of the systems running this software
HP-UX	Yes	Yes	Mostly, or on approximately 81-95% of the systems running this software
Linux	No	Yes	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: SSA is in the upper level of this range for Solaris and HP-UX. The significant risk items for these systems should be addressed by September 20, 2005 according to the Agency. Additionally, Linux is not the operating system for any of SSA's 20 Major Applications or General Support Systems, but Linux was deployed on a limited number of personal computers connected to SSA's network for the past several years. Upon discovery of this system, SSA OCIO granted an exception waiver in August 2005 to allow the use of this operating system on a temporary basis. It is anticipated the Linux operating system will be removed from these computers by September 30, 2005.

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:		

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[1]

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

[1] SSA is in the upper level of this range.

Appendix C

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.[1] Since 1997, the Social Security Administration (SSA) has had an internal controls reportable condition concerning its protection of information.[2] The resolution of this reportable condition remains a priority for the Agency. SSA is working with the Office of the Inspector General (OIG) and PricewaterhouseCoopers LLP (PwC) to develop an approach to resolve this reportable condition and other issues that were observed during the past FISMA reviews.

In August 2001, the President's Management Agenda (PMA) was initiated to improve the management and performance of Government. The PMA's guiding principles are that Government services should be citizen-centered, results-oriented, and market based. The Office of Management and Budget (OMB) developed a traffic light scorecard to show the progress agencies made: green for success, yellow for mixed results, and red for unsatisfactory. One of the five governmentwide initiatives is to increase the number of Government services available to the public electronically, through the Internet. This initiative is known as expanding Electronic Government or eGov. SSA's current status is yellow and its score for progress in implementing eGov services is green. FISMA requires agencies to take a risk-based, cost-effective approach to securing their information and systems, and assists Federal agencies in meeting their responsibilities under the PMA. FISMA authorizes the National Institute of Standards and Technology to develop standards for Agency systems and security programs.[3] SSA has committed significant resources on getting to green on the eGov initiative.

According to the standards of the PMA, the following five security actions must occur for an Agency to reach and maintain green on its Expanding e-Gov Scorecard:

- Submit quarterly status reports to remediate IT security weaknesses;
- Have the OIG verify the effectiveness of the Department-wide IT Security Remediation Process;
- Have 100 percent of all IT systems properly secured (certified and accredited);
- Install IT systems in accordance with security configurations; and
- Consolidate and optimize all infrastructures for the Continuity of Operations Plan.[4]

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

[2] SSA's FY 2004 *Performance and Accountability Report,* page 212.

[3] Public Law 107-347, Title III, section 301, 44 U.S.C §3543 (a)(3).

[4] http://www.whitehouse.gov/results/agenda/standards.pdf as of August 18, 2005.

Scope and Methodology

The Federal Information Security Management Act (FISMA) directs each agency's Office of the Inspector General (OIG) to 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) 2005 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-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-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, National Institute of Standards and Technology guidance, 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.

As part of our evaluation, we considered the security implication of the President's Management Agenda, the Electronic Government initiative. Additionally, we reviewed SSA's FISMA Privacy Report, PwC's response to the OMB FISMA questions and the supporting documentation

The results of our FISMA evaluation are based on the PwC FY 2005 FISMA *Agreed-Upon Procedures* report and working papers, various audits and evaluations performed by this office. We also reviewed the final draft of *SSA's FY 2005 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 twenty 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 through September 2005. 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 (b)(1).

Appendix E

Systems Certified and Accredited in FY 2005

#	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	

Appendix F

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

Phil Rogofsky, Audit Manager (410) 965-9719

Acknowledgments

In addition to the persons named above:

Grace Chi, Auditor

Mary Ellen Fleischman, Senior Program Analyst

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-14-05-15060.

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 Executive Operations (OEO). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

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

Office of Investigations

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

Office of the Chief Counsel to the Inspector General

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

Office of Executive Operations

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