FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2004
Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act

A-14-04-14040

September 2004 Patrick P. O'Carroll, Jr. – Acting 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 30, 2004 Refer To:

To: The Commissioner

From: Acting Inspector General

Subject: Fiscal Year 2004 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-04-14040)

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 (FISMA) of 2002.[1] We also reviewed the Agency's efforts to reach green on the security portion of the expanded electronic Government (eGovernment) initiative of the President's Management Agenda (PMA). Our analysis included an evaluation of SSA's plan of action and milestones (POA&M), certification and accreditation (C&A), and systems inventory processes.

BACKGROUND

FISMA requires Federal agencies to create protective environments for their information systems. It does so by creating a framework, which includes annual Information Technology (IT) security reviews, vulnerability reporting, and remediation planning.[2] In August 2001, the PMA was initiated to improve the management and performance of Government by focusing on citizen-centered, results-oriented, and market-based services.

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 Government-wide PMA initiatives is to increase the number of Government services available to the public electronically, through the Internet. This initiative is known as expanded electronic Government or eGovernment. SSA's current status is yellow and its score for progress in implementing eGovernment services is green. Many of the elements of the eGovernment initiative overlap or duplicate the requirements of FISMA. See Appendix C for more background.

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

[2] Pub. L. No. 107-347, Title III, Sec. 301, § 3544.

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.[3] The OIG contracted with PricewaterhouseCoopers LLP (PwC) to audit SSA's Fiscal Year (FY) 2004 financial statements.[4] 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. These reviews followed the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual*. [5] PwC performed an "agreed-upon procedures" engagement using FISMA, OMB, 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.[6] As part of this evaluation, we also reviewed the Agency's compliance with the PMA's eGovernment initiative. See Appendix D for more details on our Scope and Methodology.

SUMMARY OF RESULTS

During our FY 2004 FISMA evaluation, we determined that SSA has generally met the requirements of FISMA and the security portion of the PMA eGovernment initiative. SSA has made improvements over the past year to further strengthen its compliance with FISMA. The Agency has worked diligently to reach green on the PMA's eGovernment initiative.

To fully meet the FISMA and PMA requirements and enhance SSA's information management in this area, SSA should:

- complete the implementation of the Automated Security Self-Evaluation and Remediation Tracking (ASSERT) system as specified in SSA's security policy and use the system to generate the POA&M reports;

- develop and enforce policies for the systems inventory to ensure the inventory is updated each year;

[3] Pub. L. No. 107-347, Title III, Sec. 301, § 3545.

[4] OIG Contract Number GS23F8126H, dated March 16, 2001. FY 2004 option was exercised on November 22, 2003.

[5] GAO *Federal Information Systems Controls Audit Manual*, *Volume I: Financial Statement Audits,* GAO/AMID-12.19.6, June 2001.

[6] OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004 and NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

- continue to ensure that C&As are properly updated every 3 years or when a significant change occurs and new C&As are prepared for any new major system;

- develop and implement a methodology to accurately track and monitor IT security training; and

- fully test its continuity of operations plan (COOP).

PRESIDENT'S MANAGEMENT AGENDA – GETTING TO GREEN

According to the standards of the PMA, to get to green on its PMA eGovernment scorecard, an agency must:

- prepare quarterly status reports that document sustained progress in remediating IT security weaknesses; **and**

- have the Inspector General verify that there is an effective Department-wide IT security remediation process; **and**

- have 90 percent of operational IT systems properly secured (certified and accredited) including mission critical systems.[7]

We reviewed SSA's remediation and C&A processes. Based on these analyses, SSA has generally met the above standards as set by the PMA.

SSA IMPLEMENTED ASSERT TO MONITOR ITS REMEDIATION PROCESS AND GENERATE POA&MS

During FY 2004, SSA implemented the ASSERT tool as the focal point of its remediation process. According to the Agency, ASSERT will monitor all security deficiencies and enable SSA to accumulate all system weaknesses and remediation steps in a single location. ASSERT features include tracking the weakness by title and source, identifying the individual responsible for resolving the weakness, and providing the status on the resolution of the weakness. SSA plans to include ASSERT policies and procedures in its *Systems Security Handbook*. Based on our review of the ASSERT tool and the assessment of the compensating manual controls currently in place until the system is fully implemented, the process generally met the OMB requirements.[8]

The Agency has input into ASSERT the remediation tasks and scheduled completion dates for the weaknesses that will be in its quarterly status report to OMB. Additionally, SSA has completed a NIST Self-Assessment for each of its major systems, which were

[7] http://www.results.gov/agenda/standards.pdf as of September 1, 2004.

[8] OMB Memorandum M-04-25, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 23, 2004, page 14.

also included in ASSERT.[9] SSA manually generated its September 15, 2004 quarterly POA&M update report; however, the December 15, 2004 quarterly POA&M update report should be automatically generated from ASSERT. The manually prepared POA&Ms were effective for tracking the weaknesses designated as reportable to OMB by SSA.

The Office of the Chief Security Officer (CSO) coordinates with other components in the Agency, specifically the Office of Finance, Assessment and Management and the Office of Systems' Office of Telecommunications and Systems Operation (OTSO) to ensure that all security weaknesses are incorporated into ASSERT. OMB guidance requires that agencies also report, "…all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial systems audits, and critical infrastructure vulnerability assessments."[10] SSA reported 13 security weaknesses to OMB in its September 2004 POA&M report. In addition, SSA is tracking over 100 other security weaknesses and their remediations that the Agency identified as non-OMB reportable.

SSA stated that remediation tasks and scheduled completion dates for all weaknesses should be input into ASSERT by December 2004. When ASSERT is fully implemented and complies with the current policies, the effectiveness of the Agency-wide IT security remediation process should be improved.

OMB guidance states that the Agency needs to meet the requirements of development, implementation, and management of an agency-wide POA&M process.[11] Based on our analysis, the ASSERT tool and the interim compensating manual controls generally met the requirements set by OMB for an effective POA&M process.

SSA IDENTIFIED ALL PROGRAMS, SYSTEMS AND SUBSYSTEMS

FISMA requires that agencies develop and maintain an inventory of major information systems.[12] Program officials and Chief Information Officers (CIO) are responsible for reviewing the security of all programs and systems under their respective control. In FY 2004, SSA completed an inventory of all programs, systems, and subsystems. SSA identified an inventory of 20 major systems, consisting of 14 general support systems and 6 major application systems, as well as over 300 subsystems. Each subsystem was listed with the corresponding system(s) it supported.

SSA's CSO used a systems inventory from its Year 2000 effort as a baseline. The Agency compared this baseline to the systems and subsystems in its National Computer Center's Business Impact Analysis and its ENDEVOR tool. ENDEVOR is an

[9] NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

[10] OMB Memorandum M-04-25, *Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004, page 14.

[11] OMB Memorandum M-04-25, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 23, 2004, page 14.

[12] Pub. L. No. 107-347, Title III, Sec. 305(c)(2).

integrated set of management tools used to control and monitor SSA's application development and production implementation processes. The Office of the CSO worked with OTSO to ensure all subsystems were included in the systems inventory and any obsolete systems were removed from the inventory. From these efforts, SSA developed its systems inventory. We reviewed the process and the systems and subsystems in the inventory. We performed limited testing of the inventory to determine whether it included all subsystems. When we brought the items that were omitted from the inventory to the Agency's attention, SSA added the items to the inventory. The inventory appears complete and no additional subsystems have come to our attention that would lead us to believe additional items were omitted from this listing. SSA plans to create a systems update policy to ensure the list is maintained and kept current. The Agency is developing an appropriate methodology to maintain the inventory.

SSA CERTIFICATION AND ACCREDITATION PROCESS APPEARS TO COMPLY WITH FISMA AND NIST GUIDANCE

NIST Special Publication (SP) 800-37 provides guidelines for the Federal Government to certify and accredit its information systems. The Publication states "Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program."[13] The security accreditation is management's approval to put a system into operation and its acceptance of any risk that will occur.[14] The security accreditation must be prepared for each major system and must include an approved system security plan, security assessment reports, and POA&Ms.[15]

SSA system managers prepared the C&A for the major systems, which included the documentation required by NIST SP 800-37. We reviewed the 20 C&As for the major systems. The C&As appear to be in compliance with NIST SP 800-37. SSA must ensure these 20 C&As are updated every 3 years or when a significant change occurs and that new C&As are prepared for any new major system. Nothing came to our attention that led us to believe 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 2004.

SSA NEEDS TO DEVELOP AN INFORMATION SECURITY TRAINING METHODOLOGY

According to FISMA and OMB guidance, agencies are required to report on the extent of security training provided during the reporting period.[16] This includes security

[13] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* May 2004, page 1.

[14] Id.

[15] Id, page 21.

[16] OMB Memorandum M-04-25, *Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004, Section G.

awareness training provided to all employees and information security training provided to employees with specialized security responsibilities. We found that SSA provides specialized security training for those employees with extensive security responsibilities and security awareness training for other employees to perform their normal duties. SSA currently accumulates this information manually to comply with FISMA. However, it is difficult to manage the security training program without a sound methodology in place.

SSA is developing a methodology to more accurately track the IT security training provided to each employee. This information should identify the title, date and cost of the training provided. The Agency decided to modify its Human Resources Management Information System to track security training, but this change is not yet complete. When a system or methodology is implemented, it is expected to enhance SSA's ability to manage its information system security training program.

SSA NEEDS TO IMPROVE ITS CONTINUITY OF OPERATIONS PLANS PROCESSES AND PROCEDURES

SSA has not fully coordinated and tested its COOP. 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.[17]

SSA continues to address its COOP issues for the entire Agency. For example, SSA participated in the Government-wide disaster recovery exercise (DRE) known as Forward Challenge. DRE gave SSA an opportunity to test its COOP at an executive level. SSA executives were involved in this exercise, but it did not flow down to the front line field workers. We determined that there are still some deficiencies and weaknesses with SSA's COOP and DRE. While detailed COOPs were completed and/or updated during FY 2004, they were not fully tested. 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 the Department of the Treasury (Treasury) and the State Disability Determination Services. In the event of a disaster, SSA is uncertain as to the availability of these agencies. SSA plans to coordinate and complete a DRE with Treasury's Financial Management Services next year.

[17] Pub. L. No. 107-347, Title III, Sec 301 § 3544(b)(8).

CONCLUSIONS AND RECOMMENDATIONS

During our FY 2004 FISMA evaluation, we determined that SSA generally met the requirements of FISMA and the security requirements of the PMA eGovernment initiative. SSA worked cooperatively with the OIG to identify ways to comply with FISMA and the eGovernment initiative. SSA has 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. Continue to ensure the ASSERT system is in compliance with the Agency's policies, and properly identifies, tracks, and reports the remediation of all system deficiencies. The ASSERT tool should generate POA&Ms which should be monitored to ensure that deficiencies are resolved.

2. Create policy to ensure that the systems inventory is maintained and accurately reflects the current systems and subsystems operated by SSA.

3. Continue to ensure that C&As are properly updated every 3 years or when a significant change occurs and new C&As are prepared for any new major system.

4. Continue to implement a methodology to track and monitor IT security training and awareness.

5. Continue to implement a complete and coordinated COOP for the Agency, which is tested on a regular basis.

Patrick P. O'Carroll, Jr.

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
CSO	Chief Security Officer
DDS	Disability Determination Services
DRE	Disaster Recovery Exercise
eGovernment	Electronic Government
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
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
OPSS	Office of Protective Security Services
OTSO	Office of Telecommunication and Systems Operations
PMA	President’s Management Agenda
POA&M	Plan of Action and Milestones
PwC	PricewaterhouseCoopers LLP
SP	Special Publication
SSA	Social Security Administration
SUMS	Social Security Unified Measurement System
Treasury	Department of the Treasury
US-CERT	United States Computer Emergency Readiness Team

Appendix B

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

A. System Inventory and Information Technology (IT) Security Performance

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency Chief Information Officers (CIO) and Inspector Generals (IG) shall each identify the total number that they reviewed as part of this evaluation in Fiscal Year (FY) 2004. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 is to be used as guidance for these reviews.

	A.1.a. **FY04 Programs**		**A.1.b.** **FY04 Systems**		**A.1.c.** **FY04 Contractor Operations or Facilities**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
SSA	8	8	20	20	6	6
Agency Total	**8**	**8**	**20**	**20**	**6**	**6**

Comments:

A.1.a. FY04 Programs
These programs are:

- Retirement insurance;
- Survivors insurance;
- Disability insurance;
- Hospital and medical insurance for the aged, disabled, and those with end-stage renal disease;
- Supplemental security income;
- Special Veterans Benefits;
- Unemployment insurance; and
- Public assistance and welfare services.

A.1.b. FY04 Systems
The Agency has identified 20 major systems and applications that are considered significant to the Agency's ability to support the Social Security Programs. All 20 systems were included in the certification and accreditation (C&A) process in FY 04. See Appendix E for a complete list of the systems and applications that the Agency considers to be critical to its ability to support the Social Security Programs.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

Bureau Name	A.2.a. Number of systems certified and accredited		A.2.b. Number of systems with security control costs integrated into the life cycle of the system		A.2.c. Number of systems for which security controls have been tested and evaluated in the last year		A.2.d. Number of systems with a contingency plan		A.2.e. Number of systems for which contingency plans have been tested	
	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
SSA	20	100 %	20	100 %	20	100 %	19	95 %	18	90 %
Agency Total	**20**	**100 %**	**20**	**100 %**	**20**	**100 %**	**19**	**95 %**	**18**	**90 %**

Comments:

A.2.a. Number of systems certified and accredited
There were 20 systems certified and accredited in FY 2004. These systems are listed in Appendix E.

A.2.d. All of the 20 major systems have contingency plans except for the Social Security Unified Measurement System (SUMS). SUMS was recently released to production.

A.2.e. All of the major systems were included in FY 2004 Disaster Recovery Exercise except SUMS and Disability Case Adjudication and Review System.

A.3. 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 Comment area provided below.

Statement	Evaluation
a. Agency program officials and the Agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Mostly, or 81-95% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Mostly, or 81-95% of the time

Statement	Evaluation
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Mostly, or 81-95% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Mostly, or 81-95% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments:

A.3.a. – SSA's Office of Protective Security Services (OPSS) is notified when new contracts are awarded to service providers and is responsible for scheduling site visits to evaluate and report on adequacy of security at the facility. OPSS also has a procedure in place that ensures that it or a sub-contractor audit firm reviews between 230 and 240 different facilities throughout the year. Such a review process follows an abbreviated form of the NIST and OMB guidelines as necessary for the facility. These reviews may include visits to SSA Field Offices and Regional Offices, State DDSs, and nongovernmental agencies. Further, the OIG performed reviews of DDSs.

A.3.b. -SSA follows NIST SP 800-26 guidelines as part of the C&A process for all significant applications and programs. The Agency uses an abbreviated form of the same NIST guidelines for those entities or facilities that the Agency has not identified as "significant."

B. Identification of Significant Deficiencies

B.1. By bureau, identify all FY04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a Plan of Action and Milestones (POA&M) has been developed. Insert rows as needed.

	FY04 Significant Deficiencies			
Bureau Name	**Total Number**	**Total Number Repeated from FY03**	**Identify and Describe Each Significant Deficiency**	**POA&M Developed? Yes or No**
Social Security Administration				
Agency Total	0	0		

Comments:

The Agency has a process in place that identifies security weaknesses noted during the course of audits and evaluations. SSA uses this information to create POA&Ms in accordance with OMB guidelines. The SSA Chief Security Officer (CSO) oversees this process and is responsible for the identification of all security findings from all audit reports or evaluations. It is the decision of the Agency to log and track in a central system, those security weaknesses that result in developing a POA&M.

In FY 2004, the Agency began the implementation of a centralized system to track security weaknesses and their resolution. The system is from SRA, Inc. and is known as Automated Security Self-Evaluation and Remediation Tracking (ASSERT). The system is based on NIST SP 800-26. This off-the-shelf system is used by Agency components responsible for the critical systems to document specific weaknesses identified during the NIST SP 800-26 review, audits, risk assessments, application reviews or any such system evaluation process. SSA will use the system to report to OMB the number and status of security weaknesses that resulted in the development of POA&Ms.

Prior to implementation of ASSERT, the Agency components completed the NIST SP 800-26 questionnaires manually and submitted them to the CIO in the C&A packages. The CIO manually prepared the POA&Ms and submitted them to OMB. With the introduction of ASSERT, the process will be electronically entered and managed. According to SSA, ASSERT is scheduled to be fully implemented and used for the preparation of the FY 2005 first quarter OMB POA&M update. ASSERT will include the components' NIST SP 800-26 questionnaires.

C. OIG Assessment of the POA&M Process

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide POA&M process. This question is for IGs only. 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 Comment area provided below.

Statement	Evaluation
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Almost Always, or 96-100% of the time
b. Program officials develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. CIO develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Almost Always, or 96-100% of the time
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always, or 96-100% of the time
Comments: See Comments to B.1 for detailed discussion of POA&M process	

C.2 OIG Assessment of the Certification and Accreditation Process Section C should only be completed by the OIG. OMB is requesting IGs assess the agency's certification and accreditation process to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST SP 800-37 should be consistent with NIST SP 800-37. This includes use of the Federal Information Processing Standards Publication 199, "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. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST SP 800-37. Agencies were not expected to use NIST SP 800-37 as guidance before it became final.

Statement	**Evaluation**
Assess the overall quality of the Agency's certification and accreditation process.	Satisfactory (generally met the requirements of FISMA, NIST, and PMA)
Comments: SSA identified 20 major applications and systems that are considered significant to the Agency's ability to support its mission. All 20 C&A managers reviewed their systems and prepared the C&A packages. The C&A packages compiled for the CIO included: ▪ Risk Assessments at least once every 3 years or before implementing a significantly modified application into production. ▪ Security Plan. ▪ Completion of the NIST SP 800-26 questionnaire. ▪ Certification by appropriate component management that the application or system complies with Federal, OMB, NIST, etc. requirements. ▪ Final sign-off for completeness of the C&A package by CIO. The Agency plans to use ASSERT to complete the NIST SP 800-26 questionnaires. Currently, the questionnaires are prepared manually.	

D. Agency-Wide Security Configuration

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agency-wide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. For example: If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

	Yes or No	**Evaluation**
D.1. Has the CIO implemented agency-wide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	**Yes**	
a. Windows XP Professional	Yes	Almost Always, or 96-100% of the time
b. Windows NT	Yes	Almost Always, or 96-100% of the time
c. Windows 2000 Professional	Yes	Almost Always, or 96-100% of the time
d. Windows 2000	Yes	Almost Always, or 96-100% of the time
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	No	Rarely, or 0-50% of the time
g. Solaris	Yes	Almost Always, or 96-100% of the time
h. HP-UX	Yes	Almost Always, or 96-100% of the time
i. Linux	N/A	Not applicable
j. Cisco Router IOS	Yes	Almost Always, or 96-100% of the time
k. Oracle	No	Rarely, or 0-50% of the time

	Yes or No	Evaluation
l.a. Other. Specify: IBM AS/400 (AIX)	Yes	Almost Always, or 96-100% of the time
l.b. Other. Specify: UNISYS (UNIX)	Yes	Rarely, or 0-50% of the time
l.c. Other. Specify: IBM zOS	No	Rarely, or 0-50% of the time

Comments:

D1.i. The Agency does not use or support Linux.

D.1.k. The Oracle application is installed and in operation on a UNIX platform. The Agency has developed a UNIX risk model.

D.1. l. The Agency supports IBM AS/400, Unisys servers, and IBM mainframes. There is a standard profile in place for AS/400 and Unisys servers, but not for the mainframes. The standard has not been consistently enforced for the Unisys hardware.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

	Yes or No	Evaluation
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	Mostly, or 81-95% of the time

Comment:

Patch management procedures address patches in multiple ways. One is to automatically implement patches to hardware through a software solution. This ensures that patches are implemented in a timely manner. The other is to make the patches available. Then, when a hardware "owner" logs onto the system from the Agency network, they are expected to identify the patches needed, download the patches, and install them at that first session.

E. Incident Detection and Handling Procedures

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Almost Always, or 96-100% of the time

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	20	100 %

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

The Agency uses a combination of automated tools, system monitoring techniques and network penetration-type reviews to identify malicious activity and security weaknesses. Some of the specific tools are as follows:

- DumpACL
- Ettercap, a packet sniffer
- Harris Stat, a vulnerability scanner
- Nmap, network port scanner and operating system identifier
- Phonesweep, a commercial wardialer
- Whisker, common gateway interface vulnerability scanner

F. Incident Reporting and Analysis

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other." If appropriate or necessary, include comments in the Comment area provided below.

	F.1. Number of Incidents, by category:		
	F.1.a. Reported internally	**F.1.b. Reported to US-CERT**	**F.1.c. Reported to law enforcement**
I. Root Compromise	0	0	0
II. User Compromise	0	0	0
III. Denial of Service Attack	0	0	0
IV. Website Defacement	0	0	0
V. Detection of Malicious Logic	0	0	0
VI. Successful Virus/Worm Introduction	0	0	0
VII. Other	0	0	0
Totals:	0	0	0

F.2 Identify the number of systems affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

	F.2. Number of systems affected, by category, on:		
	F.2.a. Systems with complete and up-to-date C&A	**F.2.b. Systems without complete and up-to-date C&A**	**F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?**
I. Root Compromise	0	0	0
II. User Compromise	0	0	0
III. Denial of Service Attack	0	0	0
IV. Website Defacement	0	0	0
V. Detection of Malicious Logic	0	0	0
VI. Successful Virus/Worm Introduction	0	0	0
VII. Other	0	0	0
Totals:	0	0	0

Comments:

There were multiple critical system scans accomplished during the course of FY 2004, including those completed by OIG during the FY 2004 Financial Statement Audit. This included scans of the computers at certain field locations during the Financial Statement Audit. SSA identified these "events" and took action to investigate and analyze them. However, SSA did not consider these events to be reportable based on the interpretation of this category, and did not include these events in any of the noted categories.

G. Training

G.1 Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST SP 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST SP 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
65,312	65,242	99.89%	345	331	95.94%	See comments	$603,695

G.2.		
	Yes or No	
a. 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	

Comments:

G.1.b Annually, SSA employees are required to acknowledge that they have read and understand the *Sanctions for Unauthorized System Access Violations* policy as their security awareness training.

G.1.e. The following is a partial list of the security-oriented courses taken by Agency staff during FY 2004 who had job duties that included significant security responsibilities:

- Active Directory;
- Auditing Your Information Security Program;
- Certified Information Systems Security Professional (CISSP) Workshop;
- Computer Security Awareness;
- Computer Security Program Manager Forum;
- Defense Against Social Engineering;
- Ethical Hacking and Assessment; and
- Focus on FISMA III Symposium.

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 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 Agenda'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 Government-wide initiatives is to increase the number of Government services available to the public electronically through the Internet. This initiative is known as expanded Electronic Government or eGovernment. SSA's current status is yellow and its score for progress in implementing eGovernment 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 reauthorized the framework laid in the Government Information Security Reform Act (GISRA), which expired in November 2002.[3] In addition to the previous GISRA requirements, FISMA authorizes the National Institute of Standards and Technology to develop standards for agency systems and security programs.[4] SSA has committed significant resources on getting to green on the eGovernment initiative.

FISMA also requires agencies to prepare and submit plan of action and milestones (POA&M) reports for all programs and systems where an IT security weakness was found.[5] The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for reported security weaknesses. POA&M reports support the effective remediation of IT security weaknesses, which is essential to achieving a mature and sound IT security program

[1] Pub. L. No. 107-347, Title III, Sec. 301, § 3544.

[2] SSA's FY 2003 *Performance and Accountability Report,* page 183.

[3] Pub. L. No. 106-398.

[4] Pub. L. No. 107-347, Title III, Sec. 301, § 3543 (a)(3).

[5] OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004, page 14.

and securing agency information and systems. FISMA now requires an OIG's evaluation of the Agency's POA&M process.[6] This evaluation is instrumental in enabling the Agency to get to green under the eGovernment scorecard of the PMA.

[6] Id., page 12.

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) 2004 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 audit 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) guidance,[2] National Institute of Standards and Technology (NIST) 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. Part of the field work included the completion of the NIST *Security Self-Assessment Guide for Information Technology Systems*.[3]

In addition, we evaluated the Agency's compliance with the President's Management Agenda, specifically, the Electronic Government initiative, and determined whether the Agency had developed, implemented, and managed an Agency-wide plan of action and milestones (POA&M) process.

The results of our FISMA evaluation were based on the PwC FY 2004 FISMA *Agreed-Upon Procedures* report and working papers, various audits and evaluations performed by the Agency, contractors including PwC, and this office. We also reviewed the final draft of *SSA's FY 2004 Security Program Review*.[4]

A major focus of our review was an evaluation of SSA's POA&M, certification and accreditation (C&A), and systems inventory processes. Our evaluation of SSA's POA&M process 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 C&As for the 20 major systems. Our review of the systems inventory process included a review of the subsystems within the new inventory and a comparison of this new inventory to other listings of Agency's subsystems.

We performed field work at SSA facilities nationwide from March through September 2004. This evaluation was performed in accordance with generally accepted government auditing standards.

[1] Pub. L. No. 107-347, Title III, Sec. 301, § 3545.

[2] OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004.

[3] NIST Special Publication 800-26 *Security Self-Assessment Guide for Information Technology Systems,* November 2001.

[4] *FY 2004 Security Program Review*, provided to our office on August 27, 2004.

Systems Certified and Accredited in FY 2004

#	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	Accelerated Electronic Disability System	AeDib
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

Al Darago, Acting Director, Data Analysis and Technology Audit Division
(410) 965-9710

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

Acknowledgments

In addition to the persons named above:

Greg Thompson, Senior Auditor

Mary Ellen Fleischman, Senior Program Analyst

Harold Hunter, Senior Auditor

Grace Chi, 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-14-04-14040.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

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 and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

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

Social Security Advisory Board

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.