FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

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

A-14-03-13046

September 2003

James G. Huse, 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 5, 2003 Refer To:

To: The Commissioner

From: Inspector General

Subject: Evaluation of Social Security Administration's Compliance with the Federal Information Security Management Act (A-14-03-13046)

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] Our analysis includes an evaluation of SSA's plan of action and milestones (POA&M) process.

SUMMARY OF RESULTS

During our Fiscal Year (FY) 2003 FISMA evaluation, we determined that SSA generally met the FISMA requirements and has made improvements over the past year. However, there are still opportunities for the Agency to strengthen its information security program. To ensure full compliance with FISMA in the future, SSA needs to address the following issues:

1. Not all system weaknesses and deficiencies were identified and reported and SSA does not have a POA&M process that tracks all significant weaknesses as specified in the OMB FISMA guidance.[2] We recommend SSA develop and implement an adequate process to identify, report, monitor, and resolve systems and security related weaknesses through the POA&M process. This process should include the ability to track all significant system weaknesses and to validate that corrective actions remedied those weaknesses. See pages 4 and 5 for more detail.

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

[2] Public Law 107-347, Title III, section 301, § 3544 (b)(6), and OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment C - section I.A.2, p. 20.

2. Not all programs, systems, and subsystems are identified and reported as specified in the FISMA guidance.[3] We recommend SSA identify all such programs, systems and subsystems. See page 6 for more details.

3. SSA does not have a complete, coordinated, and fully tested continuity of operations plan (COOP).[4] We recommend SSA work with other organizations to fully resolve this issue. See page 7 for more details.

4. The Office of Chief Information Officer (OCIO) does not have sufficient resources to manage and monitor all IT security related activities to ensure compliance with the Electronic Government (E-Government) Act of 2002.[5] We recommend SSA provide the OCIO with the necessary resources to manage all Information Technology (IT) security related activities, which would enable the Agency to comply with the E-Government Act of 2002. See page 8 for more details.

5. SSA does not adequately track and monitor all information security training.[6] We recommend SSA implement a system to track and monitor information security training. See page 9 for more details.

SCOPE AND METHODOLOGY

FISMA directs each agency's Office of 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.[7] The SSA/OIG contracted with PricewaterhouseCoopers LLP (PwC) to audit SSA's FY 2003 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 Control and 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-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, National Institute of Standards and Technology (NIST) guidance, and other

---

[3] Public Law 107-347, Title III, § 3544 (b)(3), and OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment B.I.A.2a, p. 11.

[4] Public Law 107-347, Title III, section 301, § 3544 (b)(8), and OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment A – section E, p. 7.

[5] Public Law 107-347, Title II, section 202 (f), and section 209, Title III section 301, § 3544 (a)(3)(iv), and OMB Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003, p. 4.

[6] Public Law 107-347, Title III, section 301, § 3544 (a)(4), and OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment B.I.C.3, p. 15.

[7] Public Law 107-347, Title III, section 301, § 3545 (b)(1).

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*[8] (Self-Assessment).

FISMA also requires that we evaluate the Agency's compliance with the President's Management Agenda and determine whether the Agency has developed, implemented, and managed an agency-wide POA&M process.[9]

The results of our FISMA evaluation are based on the PwC FY 2003 FISMA *Agreed-Upon Procedures* report and working papers, various audits and evaluations performed by other contractors, PwC, and this office. We also reviewed the final draft of *SSA's Annual Security Program Review Federal Information Security Management Act* FY 2003 report and the Agency's *Independent Review of Information Technology Security Program Self-Assessment* report.

We performed field work at SSA facilities nationwide from April through September 2003. The evaluations were performed in accordance with generally accepted government auditing standards.

BACKGROUND AND CURRENT SECURITY STATUS

FISMA requires agencies to create protective environments for their information systems. It does so by creating a framework for annual IT security reviews, vulnerability reporting and remediation planning.[10] Since 1997, SSA has had an internal controls reportable condition concerning its protection of information.[11] The resolution of this reportable condition remains a priority for the Agency. SSA is working with the OIG and PwC to develop an approach to resolve this reportable condition and other issues including:

- physical access controls at non-Headquarters locations, including SSA's regional offices, program service centers (PSC), and selected Disability Determination Services (DDS);

- implementation and monitoring of technical security configuration standards governing the systems housed in the National Computer Center and systems housed off-site; and

- monitoring security violations and periodic review of user access.

---

[8] *NIST Special Publication 800-26 Security Self-Assessment Guide for Information Technology Systems.*
[9] See footnote 2.
[10] See footnote 2.
[11] SSA's FY 2002 *Performance and Accountability Report,* pp. 178-9.

In August 2001, the President's Management Agenda 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. OMB developed a traffic light scorecard to show the progress agencies made: green for success, yellow for mixed results, and red for unsatisfactory. The expansion of E-Government services is one of the five government-wide initiatives assessed. SSA's current status is yellow and its score for progress in implementing E-Government 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 President's Management Agenda. FISMA reauthorized the framework laid in the Government Information Security Reform Act[12] (GISRA), which expired in November 2002. In addition to the previous GISRA requirements, FISMA authorizes NIST to development standards for Agency systems and security programs.[13]

FISMA also requires agencies to prepare and submit POA&M reports for all programs and systems where an IT security weakness was found.[14] 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 and securing agency information and systems. FISMA now requires an OIG's evaluation of the agency's POA&M process;[15] this evaluation is instrumental in enabling the agency to get to green under the expanding E-Government Scorecard of the President's Management Agenda.

SSA HAS NOT REPORTED ALL SIGNIFICANT SYSTEM DEFICIENCIES

In its FY 2003 FISMA report, SSA did not report any material weaknesses. There are, however, numerous system-related deficiencies disclosed through OIG and contractor audits, which should be reported. FISMA guidance[16] requires agencies to identify and report all material weaknesses and indicate whether POA&Ms have been developed for those weaknesses. Specifically, agencies are required to report any significant deficiencies in a policy, procedure, or practice. However, SSA has only reported those material weaknesses as defined under the Chief Financial Officers'[17] and Federal Managers' Financial Integrity Acts.[18] Based on FISMA reporting guidance,[19] SSA

---

[12] Public Law 106-398.
[13] Public Law 107-347, Title III, section 301, § 3543 (a)(3).
[14] See footnote 2.
[15] Public Law 107-347, Title III, section 301, § 3544 (b)(6).
[16] OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment A - section H, p. 8.
[17] Public Law 101-576.
[18] Public Law 97-255.
[19] OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment C - section I.A.2, p. 20.

should report all significant deficiencies in its security program and develop POA&Ms for these deficiencies.

SSA completed the NIST Self-Assessment as part of its review for FISMA FY 2003. In its Self-Assessment, SSA did not report any system weaknesses or deficiencies. In the OIG's FY 2003 completion of Self-Assessment Guide for SSA, numerous weaknesses or deficiencies were noted including:

- Inconsistencies between Windows NT risk models and the actual settings found on boxes in remote locations;
- Lack of periodic access reviews including mainframe production data; and
- Weaknesses in access controls over telecommunications hardware/facilities at PSCs and DDSs.

Presently, several components monitor and track open security and system related recommendations from contractors, General Accounting Office (GAO), and OIG reviews and audits. SSA is currently developing a database to consolidate the system-related weaknesses tracked by those different components so that it can easily determine the status of and track the remediation of its total universe of weaknesses. SSA's Chief Security Officer (CSO) anticipates that the Agency's POA&M process will use this database to identify and report on systems and security related deficiencies included in this database by the end of FY 2004.

AGENCY'S PLAN OF ACTION AND MILESTONES PROCESS DOES NOT FULLY MEET FISMA REQUIREMENTS

In June 2003, SSA management reported only eight weaknesses in the most recent quarterly update of its POA&M report. However, OMB guidance[20] 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 evaluations." Based upon all OIG, GAO, PwC, and contractor reviews and audits, there are additional weaknesses SSA should report. Examples of these weaknesses include the need to:

- Improve coordination for continuity of operations plans between the IT team and business operations;
- Establish policy and procedures to automatically remove inactive user IDs; and
- Ensure that all sensitive external transmissions are encrypted.

[20] Ibid.

According to OMB guidance,[21] Federal agencies must meet three criteria to get a score of green for security on the E-Government scorecard. Specifically, the OIG must provide a positive assertion that the agency-wide POA&M process has been improved and includes a verifiable remediation process. For SSA to improve its current status on their E-Government scorecard to green, its POA&M process needs to be implemented. Based on our evaluation, SSA's current process for monitoring weaknesses is decentralized and does not contain a method to verify remediation. SSA is in the process of building a new system related database that will meet those needs.

SSA HAS NOT IDENTIFIED ALL PROGRAMS, SYSTEMS AND SUBSYSTEMS

OMB guidance[22] requires that all agencies identify all programs, systems and subsystems, not just sensitive systems. Program officials and CIOs are responsible for reviewing the security of all programs and systems under their respective control. Such reviews are not adequate without a review of all systems supporting an agency's programs.

For the past several years, SSA has not included all programs, systems and subsystems in its Government Information Security Reform Act and FISMA reports. SSA's CSO, however, indicated that the Agency is in the process of developing a complete inventory of applications that support the Agency. The draft documentation shows a more comprehensive approach to identifying what applications are supported under the 17 sensitive systems certified annually. The Agency indicated that the project is scheduled to be completed during FY 2004. Once this list is complete, we will be able to determine whether all programs, system and sub-systems were appropriately reviewed.

---

[21] OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment B - section II.B, p. 18.

[22] OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment B.I.A, A.2a, p. 11.

SSA NEEDS TO COMPLETE ITS CONTINUITY OF OPERATION PLANS

SSA has not fully completed, coordinated, and tested its COOP. FISMA[23] 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. FISMA guidance[24] explicitly includes, in this requirement, information and information systems "…provided or managed by another agency, contractor, or other source." …For the purposes of agency implementation, "other source" has the same meaning as "other organization on behalf of an agency" discussed above."

SSA continues to improve its COOP for the entire Agency, but there are still some deficiencies and weaknesses. The COOP for mission critical systems is being developed, but is not completed. The COOP has not been tested and does not address information and information systems provided or managed by another agency, contractor or other source. SSA relies heavily upon other Federal and State government agencies such as State DDSs and the Department of Treasury but SSA is uncertain as to the availability of these agencies in the event of a disaster. Our audits have repeatedly shown that DDSs do not have adequate COOPs. The DDSs do not identify resources needed to maintain critical operations in the event of a disaster. Generally, we found that DDS COOPs have not been tested.

As another example, without Treasury's Financial Management Services (FMS), all Supplemental Security Insurance (SSI) payments would cease. FMS has mitigation efforts in place to help ensure that SSI recipients would receive their payments. However, the Treasury's FY 2002 Financial Statement report[25] includes service continuity as a material weakness. Specifically the report states that several significant deficiencies, including insufficient planning and testing, could impair timely restoration of mission critical systems, including the payment systems.[26] Without coordinating its plans with other organizations, SSA's ability to perform its mission in the event of a disaster could be greatly diminished.

---

[23] Public Law 107-347(§ 3544(b)(8)).
[24] OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment A – section E, p. 7.
[25] *Treasury's FY 2002 and 2001 Financial Statements* (OIG-03-014).
[26] Audit of *FMS' FY 2002 and 2001 Schedules of Non-Entity Government-Wide Cash* (OIG-03-039).

SSA'S OCIO'S RESPONSIBILITIES AND AUTHORITY NEEDS IMPROVEMENT TO FULLY COMPLY WITH THE E-GOVERNMENT ACT

Previously, we reported[27] weaknesses in SSA's security management structure and recommended a number of improvements including the creation of the OCIO. These recommendations were made to ensure that SSA complied with the requirements of the Computer Security Act of 1987,[28] GISRA, and the Clinger-Cohen Act of 1996.[29] Based on our recommendations, SSA created the OCIO, which restructured the information security program.

Since that report, Congress has established a wide statutory framework for IT. The E-Government Act of 2002 enhances this framework. This Act requires each Federal agency to follow information resource management policies and guidance established by OMB and developed by NIST.[30] According to OMB guidance,[31] agency Chief Information Officers (CIOs) must monitor their agency's implementation of IT standards developed by NIST. These standards include guidelines for the connection and operations between systems, categorization of Federal Government electronic information, and computer system efficiency and security.

FISMA requires that each Federal agency CIO head an office with the mission and necessary resources to ensure the agency compliance with the regulation.[32] Currently, SSA's CSO reports directly to the CIO. The CSO has a small staff that is responsible for directing and managing the Agency's enterprise information technology security program. The CSO establishes agency-wide security policies and manages the reporting and monitoring processes to ensure compliance. This is accomplished using a network of people in various locations throughout the Agency. For example, security policy is developed by one component and implemented by SSA's systems in another component. The CSO must coordinate activities with the various individuals with no direct reporting from these components. This decentralization and small staff inhibit the efficiency of the process.

We reviewed a number of Federal agencies' organizational structure and found that numerous CIOs were responsible for virtually all IT operations, including security activities. For example, within the United States Department of Health and Human Services (HHS), the CIO's office is located in the Office of Information Resources Management. The HHS CIO serves as the primary IT leader for the HHS and is responsible for developing an IT plan that lays out the Secretary's vision for enterprise architecture, consolidated systems, and strong IT security. Our review of the

---

[27] OIG report, *Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations,* June 2001 (A-13-98-12044).
[28] Public Law 100-235.
[29] Public Law 104-106.
[30] Public Law 107-347, Title II, section 202 (a)(1).
[31] OMB Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003, p. 4.
[32] Public Law 107-347, Title III § 3544 (a)(3)(iv).

Department of Veterans Affairs (VA) CIO office structure found that the VA CIO is also the Assistant Secretary for Information and Technology. The VA CIO manages the Office of Information and Technology which is responsible for a variety of functions including integrated business and IT planning, security and contingency planning, managing VA's wide area data communications network, and protecting information and privacy across VA's systems and networks. For SSA to be in full compliance with the E-Government Act, SSA's OCIO needs sufficient resources to ensure that it can manage and monitor all IT security related activities.

SSA NEEDS TO DEVELOP AN INFORMATION SECURITY TRAINING SYSTEM

According to OMB guidance,[33] agency CIO's should ensure that an appropriate IT security training program is established and operational. FISMA requires that agencies report on information security training provided employees during the reporting period. 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. However, SSA does not have a system in place that can accurately track what IT security training was provided to which employees, when the training was provided, and the cost of the training that was provided. To comply with FISMA reporting requirements, the Agency requested security training information from all components. Three components, comprising approximately 25 percent of the Agency's employee population, did not provide data that the Agency needed for FISMA reporting. Additionally, a number of components provided information on training courses that contained little or no security content. SSA has been trying to develop a training system to track security training for 3 years. The system is still not implemented. When the system is implemented, it will greatly enhance SSA's ability to manage an adequate, efficient information system security training program.

CONCLUSIONS and RECOMMENDATIONS

During our FY 2003 FISMA evaluation, we determined that SSA generally met the requirements of FISMA. SSA has developed and implemented a wide range of security policies, plans, and practices to safeguard its systems, operations, and assets. Over the years, SSA has created its OCIO, established a Critical Infrastructure Protection workgroup to oversee compliance with Presidential Decision Directive 63,[34] and implemented an incident response team.

---

[33] Implementation Guidance for the E-Government Act of 2002, M-03-18, August 1, 2003, p. 4 and OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 6, 2003, Attachment B.I.C.3, p. 15.

[34] *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63,* May 22, 1998.

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

1. Continue to develop a system to identify, track and report the resolution of all significant system deficiencies that can be used to create and monitor POA&M.

2. Clearly document and identify all programs, systems and subsystems to ensure they are reported and reviewed in compliance with FISMA.

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

4. Provide sufficient resources to permit the OCIO to ensure SSA is in full compliance with the E-Government Act.

5. Continue to develop and implement an IT security training tracking and monitoring system.

James G. Huse, Jr.

Addendum

Office of the Inspector General's Detailed Report on the Social Security Administration's Compliance with the Federal Information Security Management Act

FY 2003 Completed OMB FISMA Reporting Worksheets for SSA

A.2a[1]. Identify the total number of programs and systems in the Agency, the total number of systems and programs reviewed by the program officials and Chief Information Officers (CIOs) in Fiscal Year (FY) 03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, Inspectors General (IGs) shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.						
	FY03 Programs		**FY03 Systems**		**FY03 Contractor Operations or Facilities**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
SSA	1	1	17	17	16	16
Agency Total	1	1	17	17	16	16
b. For operations and assets under their control, have Agency program officials and the Agency CIO used appropriate methods (e.g., audits or inspections) 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 Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) policy and National Institute of Standards and Technology (NIST) guidelines, national security policy, and Agency policy?	Yes		Yes		Yes	Yes
c. If yes, what methods are used? If no, please explain why.	Audits, evaluations and assessments were completed by the Office of the Inspector General (OIG), General Accounting Office (GAO), and other audit contractors. Evaluations and surveys performed by Office of Protective Security Services and SEI.					
d. Did the Agency use the NIST Self-Assessment Guide to conduct its reviews?	Social Security Administration (SSA) completed the NIST Self-Assessment Guide for all 17 sensitive systems. However, the OIG found that the Assessment completed by the Agency did not include all system related findings. See Note 1					
e. If the Agency did not use the NIST Self-Assessment Guide and instead used an Agency-developed methodology, please confirm that all elements of the NIST Guide were addressed in the Agency methodology.	SSA used the NIST Self-Assessment Guide for all 17 sensitive systems.					
f. Provide a brief update on the Agency's work to develop an inventory of major Information Technology (IT) systems.	See Note 2					

[1] Per OMB Guidance, question A.1. only completed by the Agency.

OIG performed or participated in 71 different audits at SSA or contractor locations. These locations included SSA (38), Disability Determination Service (17), Representative Payee (7), Consulting Physicians for Disability Exams (2), OIG (2), Data Matching with Foreign Countries (1), State Bureau of Vital Statistics (1), States (1), Texas Workers Compensation (1), and Wage Reporting (1). As part of the financial statement audit, PricewaterhouseCoopers LLP (PwC) tested the following applications for the OIG during FY 2003 – Cost Accounting System, Death Alert Control & Update System, Earnings Records Maintenance System, Financial Accounting System, Integrated Client Database, Modernized Enumeration System, Modernized Claims System, Retirement, Survivors & Disability Insurance Accounting System, Retirement, Survivors & Disability Insurance Post Entitlement System, Manual Adjustment, Credit, & Award Processes, Debt Management System, Modernized Supplemental Security Income Claims System, Supplemental Security Income Records Maintenance System, Comprehensive Integrity Review Process, Office of Quality Assurance/Pre-effectuation Review, Property Accountability System, Internet Social Security Benefit Application, and FALCON Date Entry System. The audits were completed using Federal Information System Control Audit Manual standards and Generally Accepted Government Auditing Standards.
Note 1: The Agency, OIG, and GAO completed or directed completion of multiple audits at vendor and contractor locations – as documented in A2. The audit plans may or may not address all elements of the NIST Self-Assessment based on the scope and expectations of the review or assessment being accomplished.
Note 2: The Agency is in the process of developing a complete inventory of applications that support the Agency. The information is in draft at this time and not ready for release but shows a more comprehensive approach to identifying what applications are supported under the 17 Sensitive Systems that are certified annually. Currently, there were 43 additional different applications that have been initially identified. The project is scheduled to be completed during FY2004.

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether plans of action and milestones (POA&Ms) have been developed for all of the material weaknesses.				
	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
SSA	0	**See Note 1**	**See Note 1**	Yes
Agency Total	0			

Note 1: There were 3 POA&Ms carried over from FY2002. Status on all three, as of 7/3/03 was "Ongoing". Each issue had multiple parts/milestones identified that needed to be resolved before the entire issue could be closed. For issue FY02.1 there were 2 sub-tasks identified, FY02.3 - 1 sub-task, FY02.4 - 5 sub-tasks. FY02.1 subtasks noted the tasks would be completed by end of Calendar Year (CY) 04 with full resolution expected during FY04. FY02.3 indicated no change but referred to a sub-task in FY02.1 that was scheduled to be completed by end of CY04. FY02.4 sub-tasks status indicated completion in Quarter (Q) 4 FY03, end of July 2003, end of 2003, Q4 FY03, end of CY03 respectively.

The OIG found that SSA does not have POA&Ms for all weaknesses. For example, the OIG's management information system shows 40 system and security related weaknesses that may require POA&Ms to be developed.

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	**Yes**	**No**
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		See Note 1
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Yes - POA&Ms are created quarterly.	
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		See Note 1
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	Yes	
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		No - See Note 2
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) to tie the justification for IT security funds to the budget process.	Yes	
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		See Note 3
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.	Yes (see Note 1)	

Note 1: The Agency has an undocumented practice in place to develop POA&Ms based on systems and security issues identified from audits, assessments, and evaluations. SSA is developing a single database that Office of System Security Operations Management (OSSOM) will maintain and administer under the guidance of Chief Security Officer (CSO). SSA expects to complete the tracking system and database within the next few months. Once complete, the application will be used to develop the POA&M report.
Note 2: The POA&M development process is limited to those issues that the CIO deems appropriate. The Agency has other systems and processes in place to track the issues noted during audits, assessments, and evaluations. The Agency makes its own determination when these issues have been resolved.
Note 3: To date, the OIG has not been sent the POA&Ms on a regular basis. The OIG is working with the Office of the Chief Information Officer (OCIO) to improve coordination and reporting under the POA&M process.

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	SSA established the OCIO on July 11, 2002 for the CSO function, and was signed by SSA's Commissioner on July 1, 2002. The OCIO includes a separate sub-office for IT Systems Review and another for IT Security Policy. These steps are largely implemented through the Information System Security Handbook. Enforcement of the policy comes from reviews of practices through Agency, contractor, and OIG reviews and audits.
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	No - SSA policy requires such projects and investment requests to be approved by the CIO as part of the budget process.
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	SSA's System Development Life Cycle (SDLC) methodology in place (Project Resource Guide) includes a security component in each stage of any given project throughout its development and implementation (including system changes). A review of security practices and security controls is included as part of the annual Sensitive Systems Accreditation and Certification process. The annual certifications and accreditations represent specific steps taken to ensure security plans for sensitive and mission-critical systems are up-to-date and practiced throughout the systems life cycle
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please Describe.	Yes – The Agency oversees performance through the use of audits and reviews by contractors, GAO, and OIG.
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs (e.g., continuity of operations, and physical and operational security)? Please Describe.	Yes – SSA has integrated its information security program with its critical infrastructure protection (CIP) responsibilities and other security programs. SSA's CIP workgroup consists of various security personnel within the Agency that address physical security, continuity of operations, and information systems security.
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	Yes - Agency views all its security activities as falling under a single security program supported by the entire organization. Different security components are placed throughout the Agency. The components have indirect reporting links to the CSO's office (which is considered the primary security component). Security components are allocated as needed and appropriate to minimize the possibility of duplication of effort.

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets	
a. Has the agency fully identified its national critical operations and assets?	Yes
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	In process.
c. Has the agency fully identified its mission critical operations and assets?	Yes
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	In process
e. If yes, describe the steps the agency has taken as a result of the review.	Note 1
f. If no, please explain why.	N/A
Note 1: The Agency has identified eight critical assets as part of the Project Matrix Step One, and has completed vulnerability assessment for seven of the eight assets. Project Matrix Step Two reviews have been completed for five of the eight critical assets by the OIG and the Chief Infrastructure Assurance Office. Step Two review of one asset is in the draft report stage and the Step Two review of the last two assets is in the fieldwork stage.	

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?	
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	**Note 1**
b. Total number of agency components or bureaus.	1,500
c. Number of agency components with incident handling and response capability.	2 **Note 1**
d. Number of agency components that report to FedCIRC.	1
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Yes
f. What is the required average time to report to the agency and FedCIRC following an incident?	Immediately after a reportable incident has been identified
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	**Note 2**
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes
i. If yes, how many active users does the agency have for this service?	1 - SSA component Office of Telecommunication and Systems Operations (OTSO)
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	**Note 3**
k. Do these configuration requirements address patching of security vulnerabilities?	**Note 3**

Note 1: Although OTSO identifies incidents through the Incident Response Checklist and also communicates the monthly status to FedCIRC, OIG has primary responsibility to communicate such incidents to appropriate law enforcement agencies when necessary.
Note 2: OTSO has subscribed to the FedCIRC patch program but it is still in the initial implementation stage. System Software and Change Control testing in the National Computer Center accomplished in prior years noted that the Agency has a robust problem identification, validation, and implementation process that include identifying patches from multiple software vendor sites and then testing them in phases until fully confident that they resolve the problem intended. This process has been implemented to ensure that the Agency identifies patches that address weaknesses that may pose a threat to the Agency's ability to maintain a safe, sound, and secure server-based environment.
Note 3: The Agency has developed configuration standards for the AS/400, UNIX, NT, and Windows operating environments. There has not been a standard developed for any other operating environment that may be in use by ancillary locations or offices. There is an automated process in place that includes polling the AS/400's in field locations and identifying configuration anomalies and then decides whether to resolve or waive any discrepancies. If a weakness is identified that requires installation of a patch to resolve that weakness, the patch will be implemented across all appropriate domains.

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.			
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement
SSA	None	None	None

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

a. Bureau Name	b. Total Number of Systems	c. Number of systems assessed for risk and assigned a level or risk		d. Number of systems that have an up-to-date IT security plan		e. Number of systems certified and accredited		f. Number of systems with security control costs integrated into the life cycle of the system		g. Number of systems for which security controls have been tested and evaluated in the last year		h. Number of systems with a contingency plan		i. Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
SSA	17	17	100	17	100	17	100	17	100	17	100	16	94.1	14	82.4
Agency Total	17	17	100	17	100	17	100	17	100	17	100	16	94.1	14	82.4

SSA's annual system accreditations and certifications assess the risk to operations and assets under its control and determines the level of security required to protect these assets and their operations. (See Addendum I) According to SSA there are only 17 systems; however, this does not include all subsystems as required by FISMA.

According to the Federal Guidelines followed for the performance of the annual accreditations and certifications, each division or unit with responsibility for a specific sensitive system asserts that the reviews are performed in accordance with the guidance provided in NIST Special Publication 800-18 and Appendix III of OMB Circular A-130. While the accreditation assessment reports note few specific system weaknesses, they do refer to related audit reports containing identified control and security weaknesses.

Additionally, the SSA has identified its critical assets as part of the CIP process and performed assessments of risks for these assets (6 of 8) as noted in step B.4 above, to identify controls needed and levels of risk associated with the critical assets identified by the CIP. The results of these assessments are to be used to determine the level of security needed to protect these assets.

The Agency considers security in each stage of the systems development life cycle (SDLC), including system changes. This is also documented in the SDLC procedures for changes to SSA systems. Management further asserted that the review of security practices and security controls is performed as part of the annual sensitive system accreditation and certification. These annual reviews represent specific steps taken to ensure that security plans are up-to-date and continue to be practiced throughout the life cycle of each system and represent how management has maintained an up-to-date security plan for their systems. Management used outside contractors to perform independent reviews, assessments, and evaluations during FY 2003 to test and evaluate security controls and techniques. These assessments were undertaken for critical assets and are considered by the Agency to be outside of the normal audit schedule as accomplished in other divisions and operating units. These assessments were undertaken based on management's decision to obtain a different level of confirmation as to where security weaknesses may exist in the core environments.

According to SSA, two of the three systems that have not had their contingency plans tested, the Comprehensive Integrity Review Program (CIRP) and the Audit Tracking System (ATS), are deemed to be non-critical and, as such, are not required to be recovered immediately after a disaster. The third system—the LOGIPLEX building access system—has not been tested because in the event of a disaster an alternate access system, will be utilized at the recovery center. The critical sub-component of the Human Resources Management Information System (HRMIS), which is payroll, was tested as part of the disaster recovery exercise.

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.				
Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
Yes	Yes - The CIO and CSO use reports from independent audits and the OSCAR[2] reviews to assist in evaluating performance – (Also See Note 1).	Through the OSCAR and independent reviews process that periodically occur throughout the year.	Yes	No. See Note 2 & See A2 and A3 for documentation pertaining to POA&Ms and issue tracking.

Note 1: The CIO is included in the process that ensures that Agency management is made aware of the audits that are performed at and for the Agency. The process ensures that the CIO through the CSO is notified on issue resolution at least quarterly. The CIO through the CSO and OSSOM tracks components that do not complete their assessments within the previous FY. FISMA requires the agency CIOs monitor their agency's implementation of IT standards developed by NIST. At SSA, the CIO has indirect authority over security policy development and implementation. The components in charge of those activities exist in other components and are ultimately responsible to other Deputy Commissioners. OSSOM implements security policy and is part of the Office of Financial Assessment and Management and reports to the Deputy Commissioner of Finance, Assessment and Management. OTSO, which implements and monitors security policy, is part of the Office of Systems and reports to the Deputy Commissioner of Systems. Finally, FISMA requires that each Federal agency CIO head an office with the mission and necessary resources to ensure the agency compliance with the regulation. The CSO works within the office to oversee the security program, but only has a staff of three people.
Note 2: SSA develops POA&Ms based primarily on how divisions address open issues and whether or not there has been any priority to resolve them. The Agency uses other processes to log, track, and resolve issues noted during assessments. There is no centralized database to ensure that all systems and security related issues are addressed and included in POA&M.

[2] Onsite Security Control and Audit Review.

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?							
Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
64,116 (as of 8/18/03)	63,700 See Note 1	99.4% See Note 1	292	223	76%	SSA management maintains a list of course titles. See Note 2	$374,979 See Note 3

Note 1: The figure reported is based upon the number of employees who reviewed and signed their annual sanctions awareness form.

Note 2: Some of the courses reviewed did not appear to be dedicated to IT security. SSA tried to estimate how many of the courses related to IT security.

Note 3: The Agency does not have a central system for tracking security training costs. The Agency requested each component provide information on the number of people and the expense of the IT security training. SSA is currently developing a database that will centrally compile and track security training. Of the components that reported security training in FY 2003, the total costs were $374,979.

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?				
Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's capital budget for each IT investment? Y/N
SSA	None to date - not due until September. See Note 1	Yes	Yes	Yes

Note 1: The Agency has developed 16 business cases that will be submitted for FY05 cycle. Business cases for FY05 cycle are not due to be submitted to OMB until September. According to SSA, there were 20 business cases submitted in FY04 cycle.

POA&M Update – See OMB Steps A3 and D1

Quarterly POA&M Updated Information	Programs	Systems
a. Total number of weaknesses identified at the start of the quarter.	6	3
b. Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter.	1 - all others are ongoing	0 - all ongoing
c. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled.	5	3
d. Number of weaknesses for which corrective action has been delayed including a brief explanation for the delay.	0	0
e. Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.).	0	0

Note 1: The Agency has not included the date opened in the POA&Ms. Instead, it has documented the opening by identifying "How Identified" which can be tracked back to a specific event. The Agency is developing a system and process that will include identifying open dates as well as other information in accordance with NIST guidelines. To fully comply with FISMA, the new system must be able to generate POA&Ms for all issues across the Agency and it must include a verifiable remediation process. See A3 for POA&M material obtained and analyzed during the course of fieldwork.

Addendum I

Accreditations for the 17 sensitive systems reviewed for FY 2003

#	System	Acronym
1	Retirement, Survivors & Disability Insurance - Initial Claims	RSDI - IC
2	Retirement, Survivors & Disability Insurance - Post Entitlement	RSDI - PE
3	Retirement, Survivors & Disability Insurance - Accounting	RSDI - Acct
4	Recovery of Overpayments, Accounting, & Reporting System	ROAR
5	SSN Establishment & Correction System	Enumeration
6	Earnings Record Maintenance System	ERMS
7	Supplemental Security Income Records Maintenance System	SSIRMS
8	Human Resources Management Info System	HRMIS
9	Debt Management System	DMS
10	Audit Trail System	ATS
11	Death Alert Control & Update System	DACUS
12	Financial Accounting System	FACTS
13	Comprehensive Integrity Review Process	CIRP
14	Enterprise Mainframe & Distributed Network Telecom System	Network and mainframe components
15	Logiplex Security System	Logiplex
16	FALCON Data Entry System	FALCON
17	Integrated Client Database	ICDB

Appendices

APPENDIX A - Acronyms

APPENDIX B - OIG Contacts and Staff Acknowledgments

Appendix A

Acronyms

CY	Calendar Year
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COOP	Continuity of Operations Plan
CSO	Chief Security Officer
DDS	Disability Determination Services
E-Government Act	Electronic Government Act of 2002
FedCIRC	Federal Computer Incident Response Center
FISMA	Federal Information Security Management Act
FMS	Federal Management Services
FY	Fiscal Year
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
HHS	Department of Health and Human Services
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OSSOM	Office of System Security Operations and Management
OSCAR	On-site Security Control and Audit Review
OTSO	Office of Telecommunication and System Operation
PSC	Program Service Center
PwC	PricewaterhouseCoopers
POA&M	Plan of Action and Milestones
SDLC	Systems Development Life-Cycle
SSA	Social Security Administration
SSI	Supplemental Security Insurance
VA	Department of Veterans Affairs

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

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

Acknowledgments

In addition to the persons named above:

Mary Ellen Fleischman, Senior Program Analyst

Greg Hungerman, Senior Program Analyst

Harold Hunter, Senior Auditor

Greg Thompson, Auditor

Grace Chi, Auditor

Annette DeRito, Writer/Editor

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Deputy Commissioner of Social Security

Deputy Commissioner of Systems

Deputy Commissioner of Finance, Assessment and Management

Chief Information Officer

Deputy Commissioner of Operations

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

Office of Audit

The Office of Audit (OA) conducts comprehensive financial and performance audits of the Social Security Administration's (SSA) programs and makes recommendations to ensure that program objectives are achieved effectively and efficiently. Financial audits, required by the Chief Financial Officers' Act of 1990, assess whether SSA's financial statements fairly present the Agency's financial position, results of operations and cash flow. Performance audits review the economy, efficiency and effectiveness of SSA's programs. OA also conducts short-term management and program evaluations focused on issues of concern to SSA, Congress and the general public. Evaluations often focus on identifying and recommending ways to prevent and minimize program fraud and inefficiency, rather than detecting problems after they occur.

Office of Executive Operations

OEO supports the OIG by providing information resource management; systems security; and the coordination of budget, procurement, telecommunications, facilities and equipment, and human resources. In addition, this office is the focal point for the OIG's strategic planning function and the development and implementation of performance measures required by the *Government Performance and Results Act*. OEO is also responsible for performing internal reviews to ensure that OIG offices nationwide hold themselves to the same rigorous standards that we expect from SSA, as well as conducting investigations of OIG employees, when necessary. Finally, OEO administers OIG's public affairs, media, and interagency activities, coordinates responses to Congressional requests for information, and also communicates OIG's planned and current activities and their results to the Commissioner and Congress.

Office of Investigations

The Office of Investigations (OI) conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement of SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, physicians, interpreters, representative payees, third parties, and by SSA employees in the performance of their duties. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Counsel to the Inspector General

The Counsel to the Inspector General provides legal advice and counsel to the Inspector General on various matters, including: 1) statutes, regulations, legislation, and policy directives governing the administration of SSA's programs; 2) investigative procedures and techniques; and 3) legal implications and conclusions to be drawn from audit and investigative material produced by the OIG. The Counsel's office also administers the civil monetary penalty program.