FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

Fiscal Year 2009 Evaluation of the Social Security Administration's Compliance with the *Federal Information Security Management Act*

November 2009 **A-14-09-19047**

Patrick P. O'Carroll, Jr.
Inspector General

Mission

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

Authority

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

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

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

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

Vision

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

SOCIAL SECURITY

MEMORANDUM

Date: November 17, 2009 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2009 Evaluation of the Social Security Administration's Compliance with the *Federal Information Security Management Act* (A-14-09-19047)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) overall security program and practices complied with the requirements of the *Federal Information Security Management Act of 2002* (FISMA) for Fiscal Year (FY) 2009.[1]

BACKGROUND

FISMA provides the framework for securing the Government's information and information systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of their security programs. FISMA requires that each agency develop, document, and implement an agency-wide information security program.[2]

OMB uses information reported pursuant to FISMA to evaluate agency-specific and Government-wide security performance, develop the annual security report to Congress, and assist in improving and maintaining adequate agency security performance. OMB issued Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* on August 20, 2009. This year, OMB requires that agencies use an automated tool, CyberScope, to submit the annual FISMA report. See Appendix C for additional background.

SCOPE AND METHODOLOGY

FISMA directs each agency's Office of Inspector General (OIG) or an independent external auditor, as determined by the Inspector General of the agency, to perform an annual, independent evaluation of the effectiveness of the agency's information security

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

[2] Pub. L. No. 107-347, Title III, Section 301 § 3544(b), 44 U.S.C. § 3544(b).

program and practices.[3] SSA's OIG contracted with PricewaterhouseCoopers LLP (PwC) to assist in the audit of SSA's FY 2009 financial statements.[4] Because of the extensive internal control system review that is completed as part of that work, the OIG FISMA requirements were incorporated into PwC's financial statement information technology (IT) related work. This evaluation included reviews of SSA's mission-critical sensitive systems as described in the Government Accountability Office's *Federal Information System Controls Audit Manual* (FISCAM). PwC performed an "agreed-upon procedures" engagement using FISMA, OMB, National Institute of Standards and Technology (NIST) guidance, FISCAM, and other relevant security laws and regulations as a framework to complete the required OIG review of SSA's information security program, practices, and sensitive systems. See Appendix D for more details on our Scope and Methodology.

SUMMARY OF RESULTS

Based on the results of OIG and PwC's work, we determined that SSA generally complied with FISMA requirements for FY 2009; however, there are areas that need improvement. SSA continues to work toward maintaining a secure environment for its information and systems. For example, SSA continues to have sound processes in a number of areas including certification and accreditation (C&A), configuration management, privacy, and system inventory.

Although the Agency continues to protect its information and systems, our FY 2009 financial statement audit identified a significant deficiency in the Agency's controls over access to its information. SSA did not continually assess individuals' access to the Agency's mainframe information. It should be noted that a financial statement significant deficiency in internal controls does not necessarily rise to the level of a significant deficiency as defined under FISMA.[5] The FY 2009 financial statement audit significant deficiency does not rise to the level of a significant deficiency defined under FISMA because of other compensating controls the Agency has in place, such as

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

[4] OIG Contract Number GS-23F-0165N, March 16, 2001. FY 2009 option was exercised in December 2008.

[5] Government Accountability Office, Government Auditing Standards, section 5.11: A significant deficiency with regard to financial audits is defined as a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with Generally Accepted Accounting Principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. OMB *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* August 20, 2009, page 9 states a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near immediate corrective action must be taken.

intrusion detection systems, guards, closed circuit televisions, automated systems checks, configuration management, and firewalls.

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

- implementation of OIG's computer security program audit recommendations;
- implementation of effective system access controls;
- effective strategic planning that addresses future processing needs;
- protection of personally identifiable information (PII);
- full implementation of its vulnerability remediation policy;
- employees and contractors receive security awareness and specialized security training;
- proper incident handling and notification; and
- continued improvements in its C&A security assessments.

IMPLEMENTATION OF OIG COMPUTER SECURITY PROGRAM RECOMMENDATIONS

According to FISMA, each agency is required to implement an agency-wide information security program ". . . to provide information security for the information and information systems that support the operations and assets of the agency."[6] The Chief Information Officer (CIO) is responsible for ensuring agency compliance with FISMA and designating a senior agency information security officer to head an office with the mission and resources to assist the CIO in ensuring agency compliance with FISMA.[7] In September 2009, we completed a follow-up audit of our 2001 review of SSA's computer security program.[8] We found that SSA continued to have a decentralized/ fragmented information security management structure. We also found that the Office of the CIO did not have sufficient delegated authority and resources to carry out its responsibilities for SSA's information security program. To help ensure an effective security program, SSA needs to have a centralized security structure with sufficient delegated authority and resources. Further, SSA needs to have all staff responsible for developing an agency-wide security policy report to the CIO. Had SSA implemented the recommendations from our June 2001 report,[9] some of the findings discussed in this report may not have occurred.

[6] Pub. L. No. 107-347, Title III, Section 301(b)(1) § 3544(b), 44 U.S.C. § 3544(b).

[7] Pub. L. No. 107-347, Title III, Section 301(b)(1) § 3544(a)(3), 44 U.S.C. § 3544(a)(3).

[8] *Follow-up: The Social Security Administration's Computer Security Program Compliance* (A-14-09-19048) September 24, 2009.

[9] *Management Advisory Report - Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations* (A-13-98-12044), June 14, 2001.

IMPLEMENTATION OF EFFECTIVE SYSTEM ACCESS CONTROLS

OMB Circular A-123 Significant Deficiency

Controlling and limiting access to the Agency's information systems and resources is the first line of defense in ensuring the confidentiality, integrity, and availability of the Agency's information resources.[10] Lack of adequate access controls compromises the completeness, accuracy, and validity of the information in the systems.

Our audit of SSA's FY 1997 financial statements identified access controls as a reportable condition.[11] Since 1997, SSA has worked to establish sufficient access controls, as evidenced by the use of TOP SECRET software and the initiation of the Standardized Security Profile Project (SSPP).[12] Further, the Agency made significant progress identifying and establishing a baseline for security access to its financially significant mainframe applications, security administration tools, and operating systems. As a result, in FY 2005, the access control issue was removed as a reportable condition.

However, our FY 2009 financial statement audit identified a significant deficiency[13] in the Agency's control of access to its sensitive information. SSA needs to periodically recertify individuals' security accesses to Agency mainframe computers. Moreover, a policy had not been established and consistently implemented agency-wide to periodically reassess the content of security access to ensure that employees and contractors are given least-privilege accesses for their job responsibilities. Further, SSA was unable to consistently provide evidence that Agency management reviewed security accesses or "profiles"[14] to determine whether system data, transactions, and resources for financially significant applications, systems, and related tools were in line with the concept of least privilege.

Local Profiles

SSA used local profiles to allow quick changes to access rights. These changes can only occur for access that the component security officers can administer. Local profiles are not included in the TOP SECRET tracking (TSTRAC) process. The TSTRAC process is a sequence of SSA "checks and balances" for requesting, obtaining, and changing access to protect SSA data, applications, and resources. During the financial

[10] Information Systems Security Handbook, Section 2.1.

[11] A reportable condition is a control deficiency or combination of control deficiencies that in management's judgment represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet its internal control objectives.

[12] SSPP is a project to ensure programmers only have the least system privilege.

[13] See Footnote 5.

[14] A profile is one of TOP SECRET's primary access control mechanisms. Each profile contains a unique mix of facilities and transactions that determines what access to systems resources that specific position needs.

statement audit, approximately 3,650 local profiles were identified. We identified 101 of the 3,650 local profiles as having access to financially significant applications. Our tests found that the Agency had not been properly managing and monitoring these 101 local profiles. Our testing on non-financially significant local profiles was limited. We plan to expand our review in FY 2010 to determine whether these profiles have any significant impact on SSA's non-financial systems.

Other Access Control Weaknesses

SSA should continue to work to strengthen access controls in other areas. Our audit work in FYs 2007 through 2009 identified a need for SSA to strengthen employment suitability checks for SSA contractor personnel.[15] For example, we found that a number of contractor staff did not receive background checks. Therefore, these individuals should not have been permitted to work on-site at an SSA facility or have access to Agency program or sensitive information. Additionally, we determined that certain programmers had excessive access to production data for specific SSA systems. SSA should ensure that individuals only have access to the systems that are necessary to perform their jobs. As a result of these weaknesses, SSA's sensitive data could have been compromised.

A strong security plan is required as SSA increases dependence on the Internet and Web-based applications to serve the American public. Additionally, SSA needs to improve its review and assignment of access to sensitive information systems and the data contained therein. Further, SSA management should implement a policy that requires annual reviews of the assignment of profiles and the content of these profiles. The scope of the policy should include all profiles, and the process should be consistent and auditable.

EFFECTIVE STRATEGIC PLANNING THAT ADDRESSES FUTURE PROCESSING NEEDS

Effective strategic planning is critical to SSA's ability to address future processing needs and protect its sensitive data. Several OIG reports have identified a need for SSA to improve its IT long-term strategic planning.[16] SSA's IT strategic planning documents are task-oriented in nature and need to be more strategic. If SSA had a long-term and

[15] *The Social Security Administration's Information Technology Maintenance and Local Area Network Relocation Contract* (A-14-07-17022), May 21, 2007; *The Social Security Administration's Enterprise-Wide Network Infrastructure Contract* (A-14-08-18014), September 2, 2008; and *The Social Security Administration's Oversight of MDRC Contract No. SS00-06-60075* (A-15-08-18010), December 22, 2008.

[16] *The Social Security Administration's Information Resources Management Strategic Plan* (A-14-07-27133), September 28, 2007; *Quick Response Evaluation: The Social Security Administration's Ability to Address Future Processing Requirements* (A-44-09-19098), March 16, 2009; *Quick Response Evaluation: The Social Security Administration's Disaster Recovery Process* (A-14-09-29139), June 5, 2009; *Congressional Response Report: The Social Security Administration's Information Technology Strategic Planning* (A-44-09-29120), June 29, 2009; and *Processing Capacity of the Social Security Administration's Durham Support Center* (A-14-09-19100), September 30, 2009.

comprehensive IT Strategic Planning process in place, the significant infrastructure and electrical capacity issues currently affecting the National Computer Center (NCC) may have been avoided. Further, the current NCC replacement effort would not be an exercise in crisis management. Because of the significant infrastructure and electrical capacity issues, the Agency's ability to deliver services to the American public is at risk. The *American Recovery and Reinvestment Act of 2009* provided SSA $500 million to replace the NCC.[17] Proper long-term and comprehensive strategic planning will help SSA ensure the NCC replacement meets its near- and long-term needs.

In addition to the NCC replacement, SSA needs to address its ability to recover critical data processing operations in the event of disaster. The Agency's goal is to restore critical functions within 24 hours of a disaster. Currently, it will take SSA approximately 10 days to reach 34 percent of its production capacity. SSA's current disaster recovery plan is heavily dependent on the availability of a contracted facility that is available on a first-come, first-served basis. SSA has constructed a second data center, known as the Durham Support Center (DSC). The current plan shows the DSC to be fully functional[18] in 2013; however, we were advised that steps have been taken to ensure the DSC will have the mainframe capacity to perform all critical NCC workloads[19] by 2010. The DSC would prove to be an important option should the NCC be affected by a catastrophic event that affects the Northeast region. Our FY 2009 reviews recommended that SSA accelerate the use of the DSC as a fully functioning data center—with particular emphasis on using the DSC as the disaster recovery site for the NCC.[20]

[17] Pub. L. No. 111-5, Division A, Title VIII, H.R. 1-71.

[18] A data center is fully functional when it will process a portion of SSA's critical and non-critical workloads. Each data center will back up the data assets of the other. The centers will be designed so that, in the event of a disaster, the critical workloads of one will be assumed by the other. Non-critical workloads will be deferred until the impacted center is restored to full operations or the capacity of the unaffected center can be expanded.

[19] SSA's critical workloads are enumeration and claims administration for benefits and post-entitlements under Titles II and XVI.

[20] *Quick Response Evaluation: The Social Security Administration's Disaster Recovery Process* (A-14-09-29139), February 17, 2009 and *Processing Capacity of the Social Security Administration's Durham Support Center* (A-14-09-19100), September 30, 2009.

PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

OMB has issued guidance[21] on how Federal agencies should safeguard PII.[22] For example, the current FISMA reporting guidance[23] requires that SSA include the following items as an appendix to its annual FISMA report:

- breach notification policy, if it has changed significantly since last year's report;
- progress update on eliminating unnecessary use of Social Security numbers (SSN); and
- progress update on review and reduction of holdings of PII.

SSA has taken various steps to safeguard PII. It created a PII Portal Website that defined SSA managers' and employees' responsibilities to ensure the confidentiality of the information they collect and hold. SSA also established a PII Executive Steering Committee to provide oversight as well as make recommendations on Agency PII policy to the Commissioner as well as other groups to oversee the public Internet site and internal Intranet sites. For example, the Agency established the Web Steering Committee to facilitate coordination between responsible components on the development, management, and maintenance of its Internet site. In addition, SSA established the Internet and Intranet Application Standards Workgroups to oversee the Internet and Intranet sites.

SSA can still improve its efforts to protect PII. For example, we identified instances of PII on the Agency's Intranet.[24] SSA has attempted to mitigate these PII breaches by removing the PII from the public domain. However, our search of SSA's Intranet sites detected 179 instances of PII being displayed. We found most of this PII on regional Intranet sites maintained by SSA's Office of Disability Adjudication and Review. In addition, we found 11 other instances of exposed PII on other SSA Intranet sites containing Agency training manuals. After we notified SSA officials about the exposed PII, it was immediately removed from the Intranet sites.

We reported that the Agency lacked a designated component to monitor PII issues related to SSA's Internet and Intranet sites. Moreover, SSA had not developed clear

[21] OMB Memorandum M-09-29, supra at cover pages; OMB Memorandums M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*, January 18 2008; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007; and M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

[22] PII refers to information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, biometric records etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual such as date and place of birth, or mother's maiden name.

[23] OMB Memorandum M-09-29, supra at cover pages.

[24] *Protecting Personally Identifiable Information on the Social Security Administration's Intranet Sites* (A-12-09-29118), August 19, 2009.

and relevant content standards for safeguarding PII on its Websites. SSA's lack of controls may have contributed to PII being displayed on the Agency's Intranet sites. SSA should ensure that controls to protect PII are fully developed and implemented in accordance with OMB guidance.

FULL IMPLEMENTATION OF SSA'S VULNERABILITY REMEDIATION POLICY

FISMA requires that agencies implement an information security program that includes a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the Agency's information security policies, procedures, and practices.[25] OMB requires that agencies have a Plan of Action and Milestones (POA&M) process to manage their remediation of security vulnerabilities.[26] In FY 2009, SSA implemented a new automated system called Cyber Security Assessment and Management, to manage its remediation process. SSA has an adequate remediation policy, but the policy has not been fully implemented. For example, some of the deficiencies in the Agency's information security policies, procedures, and practices were not tracked by Cyber Security Assessment and Management, and some Agency component quarterly remediation status reports were not provided to the Office of the CIO. We also found some deficiencies were not remediated timely. SSA should strengthen its POA&M process to ensure all deficiencies are tracked and appropriately addressed timely. Further, Agency components should provide timely remediation status reports to the Office of the CIO as required by Agency policy.[27]

ENSURE EMPLOYEES AND CONTRACTORS RECEIVE SECURITY AWARENESS AND SPECIALIZED SECURITY TRAINING

FISMA and OMB require that all Agency personnel and contractors receive appropriate annual security awareness and specialized security training.[28] The Agency states that its approach to providing information security training to all SSA employees and system users follows the guidelines in *OMB Circular A-130, Appendix III,*[29] which indicates that

[25] Pub. L. No. 107-347, Title III, Section 301(b) § 3544(b)(6), 44 U.S.C. § 3544(b)(6).

[26] OMB M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.

[27] Information Systems Security Handbook, Appendix U.

[28] OMB M-09-29, supra at page 17, states "…the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., user awareness training and training on agency policy and procedures)." Pub. L. No. 107-347, Title III, Section 301(b) § 3544(a)(4) requires each agency head to ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines. OMB M-07-16, Attachment 1 § A.2.d states "Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities... Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties."

[29] Section A.3.a.2.b.

all individuals must be appropriately trained to fulfill their security responsibilities before they are granted access to agency systems. FISMA requires that each agency develop, document, and implement an agency-wide information security program.[30] NIST recommends agencies monitor the compliance and effectiveness of their security awareness training programs.[31] An automated tracking system should be designed to capture key information regarding program activity (for example, courses, dates, audience, costs, and sources). The tracking system should capture these data at an agency level, so they can be used to provide enterprise-wide analysis and reporting regarding awareness, training, and education initiatives.[32]

We found that SSA's security awareness and training program had two deficiencies:

1. SSA did not have an effective process to confirm that all users with log-in privileges completed annual security awareness training before accessing the Agency's systems.
2. SSA did not have an effective process to monitor compliance and effectiveness of the security awareness and specialized security training program.

SSA could not provide sufficient documentation to support that its employees and contractors completed the required security awareness and specialized security training before accessing the Agency's systems. Moreover, SSA stated that all employees and contractor personnel received appropriate security awareness and security training. However, Agency staff could only provide evidence that 16 of 45 users in our sample received specialized training. We also found that some contractors were provided access to SSA's systems before they received the security awareness statement. We recommend SSA develop a system or process that adequately confirms all users with log-in privileges complete annual security awareness training. Further, SSA needs to establish an automated tracking system to create, review, and maintain security awareness training records for all employees and contractors as evidence of compliance with OMB A-130, FISMA, and NIST guidelines.

ENSURE PROPER INCIDENT HANDLING AND NOTIFICATION

SSA only reported 35 percent of the PII incidents to US-CERT within 1 hour. OMB requires that agencies report all PII incidents within 1 hour of detection without distinguishing between suspected and confirmed breaches.[33] SSA management said it strives to comply with the OMB timeframes; however, SSA conducts additional research

[30] Pub. L. No. 107-347, Title III, Section 301(b) § 3544(b), 44 U.S.C. § 3544(b).

[31] NIST Special Publication (SP) 800-50 *Building an Information Technology Security Awareness and Training Program*, October 2003, page ES-1 states "Within agency IT security program policy, there must exist clear requirements for the awareness and training program."

[32] NIST 800-50, supra at section 6.1.

[33] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

to confirm the PII incident actually occurred. As a result, valuable time is lost before law enforcement agencies and US-CERT are notified and can begin their investigations. Further, since SSA waits to confirm a PII incident instead of immediately reporting a suspected PII incident, the Agency is not in compliance with OMB policy.[34]

In addition, FISMA requires that agencies notify and consult with law enforcement agencies and their OIGs regarding security incidents, as appropriate.[35] Further, SSA's Administrative Instructions Manual System (AIMS) states that ". . . In the event of loss, theft or damage to SSA controlled personal property; employees are to report promptly to the appropriate custodial officer, through their immediate supervisor."[36] In FY 2009, SSA reported that 37 incidents were reported to law enforcement. The custodial officers notify building security, Federal Protective Service, and/or local police of suspected thefts.[37] We sampled 5 of the 37 incidents reported to law enforcement and found that OIG did not receive notice of the 5 incidents; however, the Agency's Change, Asset, and Problem Reporting System showed that all 5 incidents were forwarded to law enforcement agencies. We did not contact other law enforcement agencies to verify whether the five sampled incidents were reported.

SSA needs to comply with OMB Memorandum M-06-19[38] and ensure proper handling of security incidents from the time of detection to final resolution.

[34] Id.

[35] Pub. L. No. 107-347, Title III, Section 301 (b)(1) § 3544 (b)(7)(C)(i), 44 U.S.C. § 3544 (b)(7)(C)(i).

[36] Administrative Instruction Manual System, Materiel Resources Manual, Chapter 4 Property Management, Section 04.05.05 A.

[37] AIMS, supra at section 04.05.05 B.2.

[38] See Footnote 34.

CONTINUED IMPROVEMENTS IN C&A SECURITY ASSESSMENTS

SSA conducted C&A reviews[39] for its 20 major systems in the past 3 years, as required by FISMA.[40] To test SSA's compliance with OMB[41] and NIST guidance,[42] we reviewed 4 of the 10 systems certified in FY 2009. We found SSA's C&A process generally met the requirements of NIST SP 800-37.[43]

Although SSA generally met the Federal requirements for C&As, it needs to improve the security assessment process to ensure security weaknesses are identified. As reported in our FY 2008 FISMA assessment, SSA's security assessments were largely based on less effective assessment methods, such as examinations and interviews.[44] SSA made some improvements during the FY 2009 C&A process by significantly increasing the use of the test method[45] to assess the effectiveness of its security controls. However, there were weaknesses relating to access control, contingency planning, and other areas tested that should have been identified in the C&A review process. We recommend SSA continue to improve its C&A process by increasing the usage of the test assessment method.

[39] According to NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004, security *certification* is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security *accreditation* is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

[40] OMB Memorandum M-09-29, page 11, states "C&A is required for all Federal information systems." This OMB guidance also indicates that section 3544(b)(3) of FISMA refers to "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems" and does not distinguish between major or other applications.

[41] OMB Memorandum M-09-29, supra, FY 2009 FISMA Reporting, Annual FISMA Reporting Inspector General Questions, Question 5.

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

[43] Id.

[44] NIST SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems,* July 2008, page 9, defined 3 security control assessment methods: examine, interview and test. The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects. The *interview* method is the process of conducting discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence. The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

[45] Id.

CONCLUSIONS AND RECOMMENDATIONS

Our FY 2009 FISMA evaluation determined that SSA generally complied with FISMA; however, some improvements are needed. SSA worked with us to identify ways to comply with FISMA. The Agency continues to develop, implement, and operate security controls to protect its sensitive data, assets and operations.

In our prior reports, we identified similar issues related to SSA's (1) computer security program, (2) access controls, (3) strategic planning, (4) protection of PII, (5) vulnerability remediation process, (6) employee and contractor security awareness training, (7) incident reporting, and (8) C&A process. We affirm our prior recommendations in these areas and encourage the Agency to fully implement these recommendations.

SSA should continue to strengthen its overall security program and practices and ensure future compliance with FISMA and other information security related laws and regulations; therefore, we recommend SSA:

1. Ensure system access controls are fully implemented to meet least privilege criteria for all users of SSA's systems. This includes regular monitoring of access to SSA's systems.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

AIMS	Administrative Instructions Manual System
C&A	Certification and Accreditation
CIO	Chief Information Officer
DSC	Durham Support Center
FIPS	Federal Information Processing Standard
FISCAM	*Federal Information System Controls Audit Manual*
FISMA	*Federal Information Security Management Act of 2002*
FY	Fiscal Year
IT	Information Technology
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
POA&M	Plan of Action and Milestones
PwC	PricewaterhouseCoopers LLP
SP	Special Publication
SSA	Social Security Administration
SSN	Social Security Number
SSPP	Standardized Security Profile Project
TSTRAC	TOP SECRET Tracking
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Appendix B

Office of the Inspector General Response to Annual *Federal Information Security Management Act of 2002* Reporting Inspector General Questions

Annual FISMA Reporting Inspector General Questions

Agency Name: Social Security Administration

Submission date: 11/18/09

Question 1: FISMA Systems Inventory

Identify the number of Agency and Contractor systems by component and FIPS 199 impact level (low, moderate, high) reviewed.

		a. **Agency Systems**		**b.** **Contractor Systems**		**c.** **Total Number of Systems (Agency and Contractor systems)**	
Social Security Administration	**FIPS 199 System Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Total Number Reviewed
Agency Totals	High	0	0	0	0	0	0
	Moderate	10	10	0	0	10	10
	Low	10	10	0	0	10	10
	Not Categorized	0	0	0	0	0	0
	Total	**20**	**20**	**0**	**0**	**20**	**20**

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

For the Total Number of Reviewed Systems Identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		a. **Number of systems certified and accredited**	**b.** **Number of systems for which security controls have been tested and reviewed in the past year**	**c.** **Number of systems which contingency plans have been tested in accordance with policy**
Social Security Administration	**FIPS 199 System Impact Level**	Total Number	Total Number	Total Number
	High	0	0	0
	Moderate	10	10	9
	Low	10	10	10
	Not Categorized	0	0	0
Agency Totals	**Total**	**20**	**20**	**19**

The Security Management Access Control System was not included in the Agency's annual Disaster Recovery Exercise.

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and Agency policy.

Agencies are responsible for ensuring the security of information systems used by a contractor of their Agency or other organization on behalf of their Agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal Agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

3a.	Does the Agency have policies for oversight of contractors?		Yes
	3a(1).	Is the policy implemented?	Yes
3b.	Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency?		Yes
3c.	Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency?		Yes
3d.	Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency?		Yes
3e.	The Agency inventory is maintained and updated at least annually.		Yes
3f.	The IG generally agrees with the CIO on the number of Agency-owned systems.		Yes
3g.	The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency.		Yes

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the Agency has developed, implemented, and is managing an Agency-wide Plan of Action and Milestones (POA&M) process:

4a.	Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?	Yes
	4a(1). Has the Agency fully implemented the policy?	No - The policy was implemented, but weaknesses were identified.
4b.	Is the Agency currently managing and operating a POA&M process?	Yes
4c.	Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the Agency or by a contractor of the Agency or other organization on behalf of the Agency?	Yes
4d.	Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?	Yes
4e.	When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?	Yes
4f.	For Systems Reviewed:	
	4f(1). Are deficiencies tracked and remediated in a timely manner?	No - We identified vulnerabilities that were not addressed timely.
	4f(2). Are the remediation plans effective for correcting the security weakness?	No – SSA’s tracking system did not provide sufficient information on how vulnerabilities were corrected. We could not conclude whether the Agency’s remediation plans for the items we reviewed were effective.
	4f(3). Are the estimated dates for remediation reasonable and adhered to?	No - We found some remediation plans were marked as delayed or not started as the plans approached its completion date. We also found some remediation plans did not contain completion dates.

4g.	Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?	No – The Agency could not provide evidence that some Program officials reported progress on security weakness remediation on a quarterly basis.
4h.	Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?	Yes

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the Agency's Certification and Accreditation (C&A) process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for C&A work initiated after May 2004. This includes use of the FIPS 199 (February 2004) "Standards for Security Categorization of Federal Information and Information Systems," to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Provide explanatory detail in the area provided.

5a.	Has the Agency developed and documented an adequate policy for establishing a C&A process that follows the NIST framework?	Yes	
5b.	Is the Agency currently managing and operating a C&A process in compliance with its policies?	Yes	
5c.	For Systems reviewed, does the C&A process adequately provide:	5c(1). Appropriate risk categories	Yes
		5c(2). Adequate risk assessments	Yes
		5c(3). Selection of appropriate controls	Yes
		5c(4). Adequate testing of controls	Yes
		5c(5). Regular monitoring of system risks and the adequacy of controls	Yes
5d.	For systems reviewed, is the Authorizing Official (AO) presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate (ATO) decision based on risks and controls implemented?	Yes	

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process		
Provide a qualitative assessment of the Agency's process, as discussed in the SAOP section, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.		
6a.	Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?	Yes
6b.	Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?	Yes
6c.	Has the Agency developed and documented an adequate policy for PIAs?	Yes
6d.	Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate PIAs?	Yes
Question 7: Configuration Management		
7a.	Is there an Agency-wide security configuration policy?	Yes
7a(1).	For each OS/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy.	

OS/Platform/ System	**Implementation Status**	**Monitoring Compliance (if Policy fully implemented)**
Microsoft Windows XP Professional	Policy fully implemented What tools and techniques is your Agency using for monitoring compliance?	

Tool/Technique/Technology	Category
System Center Configuration Manager	Configuration Scanners
System Center Configuration Manager	Patch Scanners
NESSUS; Harris STAT	Vulnerability Scanners

HP HP-UX 11	Policy fully implemented What tools and techniques is your Agency using for monitoring compliance?	

Tool/Technique/Technology	Category
CA PCM	Patch Scanners
CA PCM	Configuration Scanners
CA PCM	Vulnerability Scanners

IBM AIX 5

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
CA PCM	Patch Scanners
CA PCM	Configuration Scanners
CA PCM	Vulnerability Scanners

IBM OS390

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
SSA Developed Scripts	Configuration Scanners

Microsoft Windows Server 2003

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
System Center Configuration Manager	Patch Scanners
System Center Configuration Manager	Configuration Scanners
NESSUS; Harris STAT	Vulnerability Scanners

Oracle Database 10g

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
APP Detective	Patch Scanners
APP Detective	Configuration Scanners
APP Detective	Vulnerability Scanners

Sun Solaris 9

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
CA PCM	Patch Scanners
CA PCM	Configuration Scanners
CA PCM	Vulnerability Scanners

Sun Solaris 10

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
CA PCM	Patch Scanners
CA PCM	Configuration Scanners
CA PCM	Vulnerability Scanners

Microsoft Windows Server 2000

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
System Center Configuration Manager	Patch Scanners
System Center Configuration Manager	Configuration Scanners
NESSUS; Harris STAT	Vulnerability Scanners

Microsoft Windows Vista

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
System Center Configuration Manager	Patch Scanners
System Center Configuration Manager	Configuration Scanners
NESSUS; Harris STAT	Vulnerability Scanners

CISCO IOS 12

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

Tool/Technique/Technology	Category
SSA Developed Scripts	Patch Scanners
SSA Developed Scripts	Configuration Scanners

IBM DB2 8

Policy fully implemented

What tools and techniques is your Agency using for monitoring compliance?

No Entries

7b.	Indicate the status of the implementation of Federal Desktop Core Configuration (FDCC) at your Agency:		
	7b(1).	Agency has documented deviations from FDCC standard configuration.	Yes

	7b(2).	New Federal Acquisition Regulation 2008-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings.	No; however, the Office of Acquisition and Grants and the Office of Telecommunications and Systems Operations are collaborating to get the correct common configuration language into the contracts.
Question 8: Incident Reporting			
8a.	How often does the Agency comply with documented policies and procedures for identifying and reporting incidents internally?	90 - 100%	
8b.	How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US-CERT?	35%	
8c.	How often does the Agency comply with documented policy and procedures for reporting to law enforcement?	90% - 100%	
Question 9: Security Awareness Training			
Provide an assessment of whether the Agency has provided IT security awareness training to all users with log-in privileges, including contractors. Also provide an assessment of whether the Agency has provided appropriate training to employees with significant IT security responsibilities.			
9a.	Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log-in privileges, and providing them with suitable IT security awareness training?	Yes	
9b.	Report the following for your Agency:		
	9b(1). Total number of people with log-in privileges to Agency systems.	87,140	
	9b(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program".	74,307 – For the individuals reviewed, the Agency was unable to provide documentation to show that all individuals received security awareness training.	
	9b(3). Total number of employees with significant information security responsibilities.	325	
	9b(4). Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16,	325 – For the individuals reviewed, the Agency was unable to provide	

	“Information Technology Security Training Requirements: A Role- and Performance-Based Model”.	documentation to show that all individuals received specialized security training.
Question 10: Peer-to-Peer File Sharing		
10.	Does the Agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other Agency-wide training?	Yes

Background and Current Security Status

The *Federal Information Security Management Act of 2002* (FISMA) requires that agencies create protective environments for their information systems. It does so by creating a framework for annual information technology (IT) security reviews, vulnerability reporting, and remediation planning, implementation, evaluation, and documentation.[1] In Fiscal Year (FY) 2005, the Social Security Administration (SSA) resolved the long-standing internal controls reportable condition concerning its protection of information.[2] However, during the FY 2009 financial statement audit, SSA's management of access to its systems was identified as a significant deficiency.[3] SSA continues to work with us and PricewaterhouseCoopers LLP to further improve the security and the protection of information and information systems and resolve other issues observed during prior FISMA reviews.

The Office of Management and Budget (OMB) continues to stress the importance of protecting the public's privacy and personally identifiable information (PII). For example, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* mandates agencies to increase efforts to reduce the use of PII collected and held. OMB Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* required that agencies provide a

- breach notification policy, if it has changed significantly since last year's report;
- progress update on eliminating unnecessary use of Social Security numbers; and
- progress update on review and reduction of holdings of PII.

[1] Pub. L. 107-347, Title III, Section 301, 44 U.S.C. § 3544(a)(1), (a)(2), and (b)(1).

[2] SSA's FY 2005 *Performance and Accountability Report,* page 164.

[3] Government Accountability Office, Government Auditing Standards, section 5.11: A significant deficiency with regard to financial audits is defined as a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with Generally Accepted Accounting Principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. OMB *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* August 20, 2009, page 9 states a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near immediate corrective action must be taken.

This report informs Congress and the public about SSA’s security performance and fulfills OMB's requirement under FISMA to submit an annual report to Congress. It provides OMB an assessment of SSA’s IT security strengths and weaknesses and a plan of action to improve performance. OMB requires that agencies use an automated tool, CyberScope, to submit the annual FISMA report.

Scope and Methodology

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency's Office of Inspector General (OIG) to perform, or have an independent external auditor perform an annual independent evaluation of the agency's information security program and practices as well as a review of an appropriate subset of agency systems.[1] We contracted with PricewaterhouseCoopers LLP (PwC) to assist with the Social Security Administration's (SSA) Fiscal Year (FY) 2009 financial statement audit. Because of the extensive internal control system work that is completed as part of that audit, our FISMA review requirements were incorporated into the PwC financial statement audit contract. This evaluation included *Federal Information System Controls Audit Manual* (FISCAM) level reviews of SSA's mission critical sensitive systems. PwC performed an "agreed-upon procedures" engagement using FISMA, Office of Management and Budget (OMB) Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, National Institute of Standards and Technology guidance, FISCAM, and other relevant security laws and regulations as a framework to complete the OIG-required review of SSA's information security program and practices and its sensitive systems. We also considered the security implications of OMB Memorandum M-07-16.

The results of our FISMA evaluation are based on our FY 2009 financial statement audit and working papers related to its agreed-upon procedures engagement as well as various audits and evaluations performed by this office. We also reviewed the final draft of the Chief Information Officer and Senior Agency Official for Privacy 2009 Annual FISMA Report.

Our major focus was an evaluation of SSA's plan of action and milestones (POA&M) process, configuration management, incident management, privacy, certifications and accreditations (C&A), security awareness and training, and systems inventory processes. Our evaluation of SSA's POA&Ms included an analysis of the C&A Web solution used by the Agency and its related policies. We also reviewed SSA's updated systems inventory and the policy for the update processes.

We performed field work at SSA facilities nationwide from March to October 2009. We considered the results of other OIG audits performed in FY 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Appendix E

The Social Security Administration's Certified and Accredited Systems

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

Appendix F

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Phil Rogofsky, Audit Manager, Information Technology Audit Division

Acknowledgments

In addition to the persons named above:

Al Darago, Lead Auditor

Grace Chi, Auditor-in-Charge

Tina Nevels, Auditor

Michael Zimmerman, Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-09-19047.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform, House of Representatives

Chairman and Ranking Minority Member, Committee on Science, House of Representatives

Chairman and Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate

Chairman and Ranking Minority Member, Committee on Commerce, Science and Transportation, U.S. Senate

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts 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 reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations 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 liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG 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. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.