OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S APPROVAL AND MONITORING OF THE USE OF SOFTWARE

October 2010 A-14-10-21082

EVALUATION REPORT

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: October 27, 2010 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Approval and Monitoring of the Use of Software (A-14-10-21082)

OBJECTIVE

Our objective was to assess the Social Security Administration's (SSA) policy and procedures for approving and monitoring software on employee and contractor computers.

BACKGROUND

The *Federal Information Security Management Act of 2002* (FISMA)[1] requires that Federal agencies develop, document, and implement an Agency-wide information security program for the information and information systems that support the agencies' operations and assets.[2] FISMA also requires that heads of Federal agencies delegate authority to the Chief Information Officer (CIO) to ensure compliance with FISMA's requirements.[3] The CIO should appoint a senior agency information security officer[4] to head an office with the mission and resources to assist in ensuring Agency compliance with FISMA.[5]

The National Institute of Standards and Technology (NIST) recommends that organizations identify what types of software installations are prohibited (for example, software that is only for personal or nongovernmental use and software that may be

[1] Pub. L. No. 107-347, Title III, 44 U.S.C. §§ 3541-3549.

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

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

[4] SSA's Chief Information Security Officer is the designated Senior Agency Information Security Officer.

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

malicious or suspect).[6] Malicious software/code or malware refers to a covertly inserted program designed to compromise the integrity of the victim's computer, data, or applications.

SSA's Information Systems Security Handbook (ISSH) states that SSA managers and users must take appropriate actions to secure and prevent the improper use, damage, or destruction of SSA hardware and software.[7] Further, the only software authorized for use on SSA computers is software purchased through the Agency-sanctioned requisition process or developed, evaluated, and documented in-house.[8] Personally owned software is prohibited on SSA computers unless its use is critical to an SSA function and there is no comparable Agency software solution.[9] In these instances, managers must submit written waiver requests with justification to the Component Security Officer (CSO).[10] When this waiver is given, the local manager is responsible for monitoring the software.[11]

The Office of Telecommunications and Systems Operations (OTSO) scans and analyzes network traffic for system vulnerabilities and exploits to ensure compliance with Agency configuration settings and software requirements. SSA uses an intrusion detection system (IDS)[12] to view network traffic in real time. When a violation is detected, the IDS sends an alert to a console that is monitored by an operator. SSA uses Threat Manager, a signature-based,[13] real-time anti-virus software to monitor workstations. Additionally, SSA uses a software package called the System Center Configuration Manager (SCCM) that keeps an inventory of all "executable"[14] files on employee or contractor Windows-based computers. OTSO staff uses this inventory to identify unauthorized software. SSA monitors about 129,000 devices every 7 days.

[6] NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Section SA-7, page F-100, August 2009.

[7] SSA's ISSH Hardware and Software Security Policy, Chapter 11, § 11.3, revised August 2009.

[8] SSA, ISSH, Chapter 11 § 11.3.2.

[9] Id.

[10] Id. The CSO is responsible for advising and working with management to ensure the implementation of Federal laws and directives and SSA security policy in their area of jurisdiction.

[11] SSA, ISSH, Chapter 11 § 11.3.2.

[12] An IDS is a combination of hardware and software products that is used to analyze network traffic passing through a single point on the network. The software analyzes the data searching for specific signatures (known patterns of traffic) of malicious intent.

[13] Signature-based detection involves searching for known malicious patterns in software programs.

[14] An executable file causes a computer ". . . to perform indicated tasks according to encoded instructions."

We obtained information for this review through interviews with SSA's staff responsible for software approval and monitoring. We reviewed relevant laws, regulations, standards, and guidelines. In addition, we obtained and reviewed SSA's current software security policy and rules of behavior. Further, we obtained software security incident data from SSA's Change, Asset, and Problem Reporting System.[15] Lastly, we requested some examples of software security incidents detected through the Agency's network scanning. SSA staff provided seven security incidents that occurred in November 2009.

RESULTS OF REVIEW

Based on our evaluation, we determined that SSA had a software approval and monitoring policy for employees' and contractors' use of software on Agency computers. However, we determined the Agency's software approval and monitoring policy needed improvement. In addition, we found SSA employees, managers, and contractors did not always comply with the Agency's software approval policy by obtaining a waiver before installing non-standard software.[16] Further, in all seven software-related security incidents reviewed, we determined that no documented disciplinary action had been taken against the employee for not complying with the Agency's software approval policy.[17] As indicated below, SSA determined that five of the seven incidents were unintentional and did not warrant disciplinary action. We also found SSA's monitoring of known Agency-wide software configurations was not sufficient. Moreover, we were unable to determine whether local management was effectively monitoring software because only one software waiver was submitted for approval.

SSA's Software Approval Policy Needed Improvement

For all seven security incidents reviewed, employees and contractors did not submit waivers in accordance with the ISSH[18] to Agency security offices for approval before installing non-standard software.[19] One software waiver request was submitted for

[15] The Change, Asset, and Problem Reporting System is SSA's approved product used to manage systems changes, calls, problems, and inventory.

[16] We define software not purchased through the Agency-sanctioned requisition process or not developed, evaluated, and documented in house as non-standard software.

[17] In its initial response to these concerns, SSA stated, "We will take disciplinary action if appropriate when an employee consciously installs unapproved software. If someone does so unknowingly, however, disciplinary action is probably unwarranted. In the two incidents OIG describe where the software contained Trojan horses, pg. 5, 2nd full paragraph, it does appear employees downloaded unauthorized software onto their workstations. For the remaining cases, employees did so unwittingly, and we do not believe disciplinary action was warranted. Malware is usually hidden, and often users are unaware that unauthorized software is being installed on their computer. It is inappropriate to discipline someone in most of these situations. We must judge each case on its own merits and take action accordingly."

[18] SSA, ISSH, Appendix N, supra.

[19] Security offices refer to OTSO and the Office of Electronic Information Exchange. Office of Electronic Information Exchange staff now reports to the CIO.

approval through the Office of the Chief Information Officer (OCIO). This waiver should have been approved by the appropriate security office.

The ISSH indicates that only software purchased through the Agency-sanctioned requisition process or developed, evaluated, and documented in-house is authorized for use on SSA computers.[20] Further, exceptions for use of personally owned software must be approved via the waiver request process with written justification.[21] Managers must submit waiver requests to the CSO.[22] In turn, the CSO is supposed to submit the request to SSA's security offices.[23]

The Government Accountability Office (GAO)[24] indicated in its study of leading organizations in information security management that a central management focal point successfully fulfills the challenges of implementing security practices that gain public confidence and protect Government services, privacy, and sensitive and national security information. Further, a central management focal point is key to ensuring the various activities associated with managing risks are carried out.[25]

SSA should consider revising its software approval policy to clearly indicate that software authorized by the local manager must first go through a central management focal point, such as the OCIO, as part of the waiver approval process. If SSA does not revise its software approval policy, the potential exists for software to be installed on Agency computers without proper authorization. Consequently, the risk that malicious code could compromise or delete sensitive data and impede network operations would still exist. A revised policy would help minimize this risk.

SSA Needed to Comply with and Enforce Its Software Approval Policy

For all seven security incidents reviewed, SSA employees and contractors did not comply with the Agency's software approval policy. We received documentation confirming one software waiver request[26] had been submitted to the OCIO instead of

[20] SSA, ISSH, Chapter 11 § 11.3.2.

[21] Id.

[22] Id.

[23] SSA*, Appendix N: Requests for Exception/Waiver, Attachment B: Instructions for Completing General Waiver Request Form,* *http://eis.ba.ssa.gov/ssasso/issh/appendix/appendixn.html.*

[24] GAO Executive Guide*: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68, page 3, May 1998.

[25] GAO, *Federal Information System Controls Audit Manual,* Section 3.1 Security Management (SM), SM-1.2. A Security Management Structure Has Been Established, Page 158.

[26] The waiver facilitates the need for Office of Financial Policy and Operations to print Portable Document Format (PDF) from Social Security Online Accounting and Reporting System, which runs in Unix. The only supported method of printing PDFs from UNIX is CUPS, which is freeware.

the appropriate security offices. SSA's software approval policy states that waivers should be forwarded to the appropriate CSO. In turn, the CSO should forward the waiver to the appropriate security offices[27] for approval. SSA policy does not require that the waiver be approved by a central management focal point, such as the OCIO.

For the period October 30, 2009 through September 21, 2010, SSA had approximately 197 malware incidents reported in its Change, Asset, and Problem Reporting System. The goal of malware varies from gaining unauthorized access to simply disabling a system. Malware is typically delivered through email, but Internet relay chat channels[28] and websites can also place malicious code on a system. For the approximate 18 incidents per month, an individual could have gained unauthorized access or disabled SSA's systems. However, SSA staff does monitor the Agency's system and remediates detected incidents.

Agency staff provided seven examples of incidents where malware was installed on Agency computers, and no software waiver was submitted. Of these seven incidents, SSA determined that, in five cases, the installed software contained keyloggers,[29] and in two instances, the software contained Trojan horses.[30] These vulnerabilities were caused by the installation of non-standard software on workstations.

Non-standard software may contain malicious code (for example, viruses, worms,[31] or Trojan horses) that could infect the Agency's operating system. In addition, a Trojan horse program could be used to hijack a computer program to conduct file operations, format a disk, log keystrokes, etc. These incidents could cause SSA's network to operate inefficiently or ineffectively. Further, the malicious software could extract personally identifiable information to be used for identity theft purposes.

Although we only reviewed seven software-related security incidents, the potential for a larger issue may exist if adequate controls are not implemented to prevent the installation of unauthorized software. Further, additional controls are needed to ensure that employees submit the required waivers before installing non-standard software.

[27] SSA, ISSH, Appendix N, supra.

[28] Internet relay chat is a form of real-time Internet text messaging (chat).

[29] A keylogger application is malicious software that can capture sensitive information, such as SSA credentials or other credentials accessed from a workstation (personal email accounts, passwords, etc.) and transmit information to a third party who could gain unauthorized access to the Agency's systems or workstation user personal accounts.

[30] A Trojan horse appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.

[31] A worm is a self-replicating program that uses a network to send copies of itself to other computers on the network and may do so without user intervention. Worms usually harm the network, if only by consuming bandwidth.

For example, SSA should consider software tools that prevent unauthorized software from being installed.

The ISSH indicates that only software purchased through the Agency-sanctioned requisition process or that has been developed, evaluated, and documented in-house is authorized for use on SSA computers.[32] In addition, the ISSH indicates only SSA-authorized software may be installed on Agency devices,[33] and any exceptions involving use of personally owned software should be documented with the manager submitting a waiver in writing detailing the justification for the use of such software. If the use of non-standard software is approved, the local manager is responsible for monitoring it.[34]

Further, the ISSH[35] describes the behavior expected of all SSA personnel, contractors, and other external Government agency users of SSA's automated information systems resources. The ISSH also indicates that users must not install or use personally owned software on SSA's microcomputers unless prior management approval is obtained. Additionally, certification from SSA's Office of Information Technology Security Policy is required before using shareware and freeware on such computers.[36] Managers must ensure corrective action is taken if an infraction is discovered.[37] Noncompliance could result in one of several available penalties.[38]

We contacted the software approval offices and the managers involved with the seven incidents. We were told by the supervising managers we contacted that no documented disciplinary action had been taken against the 5 employees who unintentionally installed the non-standard software; however, the Agency agrees that appropriate disciplinary action should be taken when employees consciously install unauthorized software. SSA should consider issuing periodic reminders to managers, contractors, and employees concerning the use of non-standard software and the consequences for not complying with this policy and impose disciplinary action, when appropriate.

On June 8, 2010, the Agency issued a reminder that installation and use of unauthorized software is prohibited.

[32] SSA, ISSH, Chapter 11 § 11.3.2.

[33] Id.

[34] Id.

[35] SSA, *ISSH, Rules of Behavior for Users and Managers of SSA's Automated Information Resources (March 23, 2001)*, http://eis.ba.ssa.gov/ssasso/issh/rulesofbehavior.htm.

[36] SSA, ISSH, *Rules of Behavior, supra at Section 3.9.*

[37] Id.

[38] SSA's ISSH, *Rules of Behavior, supra at Section 4.*

SSA's Local Software Needed Monitoring

SSA had an Agency-wide software monitoring policy and process in place; however, we determined that the process was not sufficient. We received documentation confirming one software waiver request[39] had been submitted to the OCIO and not the appropriate security offices. However, SSA staff provided seven incidents where software was installed and no software waiver was submitted. Of these seven incidents, five were identified as keyloggers and two were Trojan horses. These incidents were caused by the installation of non-standard software on workstations. Since no waiver requests were submitted to the appropriate security offices, we were unable to determine whether local managers were monitoring the use of non-standard software.[40]

SSA scans and analyzes network traffic for system vulnerabilities to ensure compliance with Agency configuration and software requirements. SCCM documents employee workstation software[41] inventory. However, the Agency is limited in its monitoring efforts to identifying only malicious signatures that are known to the Agency.

SSA should consider revising its software monitoring policy to clearly indicate that OTSO has the primary responsibility for software monitoring and oversees coordination with local managers. OTSO is better equipped to identify software security incidents and related vulnerabilities. We reiterate our suggestion that the Agency issue periodic reminders to managers, contractors, and employees concerning the use of non-standard software and the consequences for not complying with this policy. In addition, the Agency should consider obtaining scanning tools that can identify malicious files other than Windows-based files.

CONCLUSION AND RECOMMENDATIONS

We found SSA had an approval and monitoring policy for employees and contractors' use of software on Agency computers. However, we determined this policy needed improvement.

Moreover, our Fiscal Year 2003 through 2009 Information Technology Management Letters cited deficiencies in workstation software monitoring and recommended SSA update its policies and procedures to timely detect and remove unlicensed and unauthorized software from workstations.

[39] SSA's ISSH, *Rules of Behavior, supra at Section 4.*

[40] See footnote 17.

[41] Microsoft Windows-based systems.

Based on our report findings, we recommend SSA:

1. Consider revising its software approval policy to clearly indicate that software authorized by the local manager must first go through a central management focal point, such as the OCIO, as part of the waiver approval process.

2. Issue periodic reminders to employees and contractors concerning the Agency's software approval and monitoring policy.

3. Enforce its software approval and monitoring policy by taking disciplinary action, where appropriate, for installing unauthorized software on Agency computers.

4. Have all software monitoring directed by OTSO with implementation by local managers.

5. Obtain electronic tools to inventory all types of software on Agency computers and prevent unauthorized software from being installed.

AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with our recommendations. The full text of SSA's comments is included in Appendix C.

Patrick P. O'Carroll, Jr.

Appendices

APPENDIX A – Acronyms

APPENDIX B – Scope and Methodology

APPENDIX C – Agency Comments

APPENDIX D – OIG Contacts and Staff Acknowledgments

Appendix A

Acronyms

CIO	Chief Information Officer
CSO	Component Security Officer
FISMA	*Federal Information Security Management Act of 2002*
GAO	Government Accountability Office
IDS	Intrusion Detection System
ISSH	Information Systems Security Handbook
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OTSO	Office of Telecommunications and Systems Operations
PDF	Portable Document Format
Pub. L. No.	Public Law Number
SCCM	System Center Configuration Manager
SM	Security Management
SP	Special Publication
SSA	Social Security Administration
U.S.C.	United States Code

Scope and Methodology

To accomplish our objective, we:

- Interviewed Social Security Administration (SSA) staff responsible for software approval and monitoring in the Agency.

- Interviewed personnel from SSA's Offices of the Chief Information Officer (OCIO) and Telecommunications and Systems Operations.

- Reviewed applicable Federal laws, directives, and other guidance as well as industry standards and best practices.

- Obtained software security incident data from SSA's Change, Asset, and Problem Reporting System.

- Requested examples of software security incidents detected through the Agency's network scanning.

- Interviewed supervisors responsible for corrective action in the event of discovered software installation infractions related to incident reports reviewed.

Specifically, we examined the:

- *Federal Information Security Management Act of 2002.*

- Government Accountability Office (GAO) *Federal Information System Controls Audit Manual*, February 2009.

- GAO *Executive Guide: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68, May 1998.

- Revisions to Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, December 21, 2004.

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53: Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

- Information Systems Security Handbook, Chapter 11: *Hardware and Software Security Policy*.

- Fiscal Year 2008 and 2009 Information Technology Management Letters.

- SSA Office of the Inspector General, *Follow-Up: The Social Security Administration's Computer Security Program Compliance (A-14-09-19048)*, September 2009.

The results of our review are based on the above information provided by SSA. We performed our review in December 2009 through September 2010 in Baltimore, Maryland. The entities reviewed were the OCIO and Deputy Commissioner for Systems. We conducted our review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspections*.[1]

[11] In January 2009, the President's Council on Integrity and Efficiency was superseded by the Council of the Inspectors General on Integrity and Efficiency, *Inspector General Reform Act of 2008*, Pub. L. No. 110-409 § 7, 5 U.S.C. App. 3 § 11.

Appendix C

Agency Comments

SOCIAL SECURITY ADMINISTRATION 75 YEARS

SOCIAL SECURITY

MEMORANDUM

Date: October 14, 2010

Refer To:

To: Patrick P. O'Carroll, Jr.
Inspector General

From: James A. Winn /s/
Executive Counselor
to the Commissioner

Subject: Office of the Inspector General (OIG) Draft Report, "The Social Security Administration's Approval and Monitoring of the Use of Software" (A-14-10-21082)—INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. Please direct staff inquiries to Rebecca Tothero, Acting Director, Audit Management and Liaison Staff at (410) 966-6975.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S APPROVAL AND MONITORING OF THE USE OF SOFTWARE" (A-14-10-21082)

Thank you for the opportunity to review the subject report. We offer the following comments.

Recommendation 1

We recommend SSA:

"consider revising its software approval policy to clearly indicate that software authorized by the local manager must first go through a central management focal point, such as the OCIO, as part of the waiver approval process. "

Response

We agree. As you discuss in footnote 22, we recently restructured the Office of the Chief Information Officer (OCIO) and it now includes the Office of Electronic Information Exchange (OEIE). OEIE retains many systems security responsibilities. We believe that by incorporating OEIO into the OCIO, we have moved towards some degree of centralization.

Recommendation 2

We recommend SSA:

"issue periodic reminders to employees and contractors concerning the Agency's software approval and monitoring policy."

Response

We agree. In July 2010, we issued a reminder that the installation and the use of unauthorized software is prohibited.

Recommendation 3

We recommend SSA:

"enforce its software approval and monitoring policy by taking disciplinary action, where appropriate, for installing unauthorized software on Agency computers."

Response

We agree. We will take disciplinary action if appropriate when an employee consciously installs unapproved software. If someone does so unknowingly, however, disciplinary action is probably unwarranted. In the two incidents OIG describe where the software contained Trojan horses, pg. 5, 2nd full paragraph, it does appear employees downloaded unauthorized software onto their workstations. For the remaining cases, employees did so unwittingly, and we do not believe disciplinary action was warranted.

Malware is usually hidden, and often users are unaware that unauthorized software is being installed on their computer. It is inappropriate to discipline someone in most of these situations. We must judge each case on its own merits and take action accordingly.

Recommendation 4

We recommend SSA:

"have all software monitoring directed by OTSO with implementation by local managers."

Response

We agree. The Office of Telecommunications and Systems Operations (OTSO) should have responsibility for monitoring infrastructure; however, we will not eliminate monitoring by local managers. We consider local managers as key in the oversight process.

Recommendation 5

We recommend SSA:

"obtain electronic tools to inventory all types of software on Agency computers and prevent unauthorized software from being installed."

Response

We agree that non-standard software may adversely affect agency operations. We will reevaluate our current policies and procedures for approving and monitoring software usage. We will also assess our current technical capabilities and identify any technology gaps.

Even with possible changes to our policies, local managers and security officers will continue to play an important role in the process and will actively participate in the approval and registration of local or non-standard software. In addition, component security staffs will continue to provide local guidance and oversight on the use of non-standard software. To enforce our policies, we must rely on component managers and security staffs. While we regularly scan our workstations and remove known malware, local managers and security officers within each component must continue their active role in the approval and oversight processes. We will maintain our efforts to prevent the introduction of malicious or destructive software onto our workstations.   At the same time, we will weigh the requirements of local managers and security officers within each component and make sure they have access to the non-standard software they need to do their work.

Appendix D

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Mary Ellen Moyer, Audit Manager

Acknowledgments

In addition to those named above:

Cheryl Dailey, Auditor-in-Charge

For additional copies of this report, please visit our Website 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-14-10-21082.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

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, Committee on the Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Oversight and Government Reform

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 Pensions and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of 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.