OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

FOLLOW-UP: THE SOCIAL SECURITY ADMINISTRATION'S ELECTRONIC MAIL SECURITY REVIEW

June 2009 A-14-09-19044

AUDIT 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: June 22, 2009 Refer To:

To: The Commissioner

From: Inspector General

Subject: Follow-up: The Social Security Administration's Electronic Mail Security Review (A-14-09-19044)

OBJECTIVE

Our objective was to determine the extent to which the Social Security Administration (SSA) implemented the recommendations from our September 2006 report, *The Social Security Administration's Electronic Mail Security Review*.

BACKGROUND

SSA has identified electronic mail (e-mail) as a critical tool to meet its mission.[1] Sensitive data are often sent via e-mail within the Agency as well as to outside entities in accordance with Agency protection of sensitive information policy.[2] Because e-mail is a popular method of exchanging data, it is also a preferred method for hackers to distribute viruses, worms, and spam as well as plan other attacks. The servers that operate an e-mail system are among the most targeted. Attackers insert software into an e-mail that infects the owner's computer and can propagate to other computers within an organization's network.[3] It is crucial that organizations protect information sent or received via e-mail from unauthorized use, disclosure, modification, destruction, or exploitation.

The day-to-day operation of the SSA e-mail system is managed by the Office of Systems' Electronic Messaging and Groupware Branch (EMGB). The SSA e-mail system is based on, and supported by, Microsoft Outlook software. Microsoft Outlook is

---

[1] Lockheed Martin's *Final Disaster Recovery Business Impact Analysis Report,* page 1, April 14, 2004.

[2] SSA's Information Systems Security Handbook, Chapter 18 requires that "Sensitive data that is to be transmitted in either direction beyond the SSA Network, (i.e., external to the firewall) must be encrypted or otherwise protected as approved by the CISO."

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-45, *Guidelines on Electronic Mail Security, September 2002,* page 1.

supported by Microsoft Exchange Server (ES) 2003. The ES server software is used to manage electronic directories and mailboxes on SSA's e-mail infrastructure.

Our September 2006 report found weaknesses in the Agency's e-mail security control framework and made nine recommendations to address them. In this review, we determined the extent to which SSA had implemented the seven recommendations with which it agreed. We also assessed the feasibility of SSA's implementation of two recommendations with which it initially disagreed.

To meet our objective, we examined various SSA policies; reviewed relevant criteria; interviewed SSA personnel; and examined the configuration settings of 17 Microsoft ES 2003 mailbox servers for compliance with Federal standards and industry best practices.[4] See Appendix B for a detailed discussion of our Scope and Methodology.

RESULTS OF REVIEW

Our 2006 report contained nine recommendations, of which the Agency agreed with seven. In our current review, we found that SSA had fully implemented four of those seven recommendations. There were two recommendations that SSA reported as implemented and closed. However, our review showed that, although the Agency had taken some corrective action, the recommendations had not been fully implemented. SSA also reported that one recommendation remains open and we confirmed its status. As a result, we believe there are four recommendations that were fully implemented, two recommendations that were partially implemented and one recommendation that remains open.

SSA disagreed with two prior recommendations. One recommendation related to disaster recovery testing and the other to conducting risk assessments. We found that, although SSA disagreed with the initial recommendation, to include e-mail in the disaster recovery testing, SSA partially implemented this recommendation. However, it was not fully implemented, because the capability to use e-mail for external communication has not been addressed.

[4] We used NIST recommended standards contained in SP 800-70, *Security Configuration Checklists Program for Information Technology (IT) Products,* May 26, 2005, to review SSA Microsoft ES 2003 configuration settings. These standards were developed by the Center for Internet Security (CIS). CIS is a nonprofit enterprise whose mission is to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.

The Agency continues to disagree with the second recommendation that an appropriate risk assessment be performed on its e-mail system. The Agency believes the Fiscal Year (FY) 2006 Agency Enterprise Wide Mainframe and Distributed Network Telecommunications Services System (EWAN) risk assessment addressed its e-mail system. However, this risk assessment did not assess the impact of the migration of the e-mail infrastructure to the Microsoft ES server 2003 platform during and after our 2006 review. Further, the SSA e-mail system has begun migration to the Microsoft ES 2007 platform, with full migration planned sometime in FY 2010. Since e-mail has not undergone risk assessments that account for significant changes to its infrastructure, SSA cannot ensure all risks have been identified and the system is secure.

It should be noted that while verifying the implementation of a prior recommendation, we found additional configuration settings that did not comply with NIST guidance.[5] In addition, an incident occurred where an e-mail administrator ignored system controls and assigned a contractor an e-mail account that already belonged to an employee. The administrator then removed the employee's account without contacting the appropriate component security officer. As a result of these newly identified issues, this report contains two new recommendations.

FULLY IMPLEMENTED RECOMMENDATIONS

Recommendation 1: Ensure that incorrect configuration settings found during our review are corrected.

SSA agreed and stated that all incorrect configuration settings identified during the 2006 review had been corrected. Our current testing of servers previously identified with incorrect configuration settings showed that those incorrect settings were corrected. We concluded this recommendation had been implemented.

Although the original incorrect configuration settings were addressed, we found additional noncompliant configuration settings. Our current testing found that each of the 17 servers tested (including 3 servers from our prior review) had at least 3 configuration settings that did not comply with NIST guidance. For example, some servers had settings that

- allowed anonymous access;
- did not set storage limits for public folders;
- were configured in a manner that did not protect the e-mail transmitted through the relay service;
- were configured in a manner that bypassed global policy involving the message size of e-mail sent and received; and
- were configured in a manner that resulted in settings that require independent rather than global management of the servers.

[5] CIS, *CIS Exchange Server 2003 Benchmark Version 1*, revised October 29, 2007.

The existence of these noncompliant configuration settings places SSA at-risk for

- inability of users to correctly authenticate access to public folders;
- public folder storage controls to be ignored;
- spammers hijacking and using relays for their own purposes;
- user noncompliance with operational policies and procedures; and
- inefficient management, excessive use of resources, and a more complex e-mail infrastructure than is necessary.

We shared these results with Agency staff who have begun addressing the noncompliant settings. We recommend SSA ensure e-mail server settings are configured correctly and in accordance with NIST guidelines.

Recommendation 4: Inform employees of their responsibility to secure information retrieved through Outlook Web Access (OWA) or the system used to access OWA.

SSA agreed and stated it had updated the message sent to OWA-enabled users to include Internet links to the SSA OWA Security and Usage Notice. Our current review found that the OWA webpage contained such a link. We concluded this recommendation had been fully implemented.

Recommendation 7: Update SSA's e-mail retention policy in the Information Systems Security Handbook (ISSH) and notify employees of the retention policies and where to find them.

SSA agreed and responded the ISSH was revised and no longer referenced e-mail retention policy but instead referred readers to the retention policy found on the Center for Records Management Intranet website. Our review of the current ISSH chapter 8 confirmed the ISSH was updated to refer employees to the appropriate source for the Agency's e-mail retention policy. We concluded this recommendation had been fully implemented.

Recommendation 9: Increase efforts to inform employees of the capabilities of the Agency's content filtering tools and post the content-filtering information in an accessible area.

SSA agreed with this recommendation and responded that it had updated content-filtering documentation on the appropriate SSA website. When this recommendation was initially made, SSA employees controlled the use of content filtering tools to manage their own e-mail accounts. The intent of the original recommendation was to provide employees with additional information to better maintain, control, and secure e-mail accounts. After our initial review, EMGB decided to centrally administer and maintain content filtering tools to control the type, size, frequency, and content of e-mail

sent and received by SSA employees. As the intent of our original recommendation has been met, we concluded this recommendation had been fully implemented.

RECOMMENDATIONS SSA AGREED WITH AND CLOSED, BUT WE DETERMINED WERE NOT FULLY IMPLEMENTED

Recommendation 2: Develop and document SSA's Microsoft ES 2003 Configuration Guide for e-mail settings in accordance with the NIST-recommended standards.

SSA agreed with our recommendation. In its response to our 2006 report, SSA indicated that it had begun developing and documenting the Microsoft ES 2003 Configuration Guide as part of its Exchange 2003 Hardening Security guidelines. Our current review found only a reference to those guidelines in an Agency document.[6] We concluded the Agency had not developed and documented its own Microsoft ES 2003 Configuration Guide.

During our current review, a procedural issue occurred where an SSA e-mail administrator incorrectly assigned the same e-mail account to an SSA contractor that was already assigned to an employee in another component. In addition, the administrator inappropriately removed the employee's e-mail account. As a control, the e-mail system generates an alert when a name is already assigned to an e-mail account. This control was ignored, and the e-mail account was assigned to a contractor without contacting the appropriate component security officer. While it appears that sensitive information may not have been disclosed in this instance, system administrators in a number of components had to spend significant time to resolve this matter. The configuration guidelines need to be finalized and include compliance with the least-privilege administrative access criteria, as well as, document the appropriate procedures for an administrator to follow. Additionally, since this employee was in a different component from the administrator, the policy should require that the administrator contact the component security officer before removing an account.

SSA's failure to update and use its own server security guidelines unnecessarily places the Agency at-risk of potentially allowing security controls to be minimized and/or compromised. We concluded that this recommendation had not been fully implemented.

Recommendation 3: Monitor Microsoft ES 2003 servers on a continuous basis for compliance with SSA's Microsoft ES 2003 Configuration Guide.

SSA agreed with this recommendation. In SSA's response to our 2006 report, the Agency indicated that server configuration audits would be conducted after the migration to the Microsoft ES 2003 platform was completed on March 15, 2008 and closed this recommendation. We found the Agency used software to monitor Microsoft

---

[6] *How to Build a Windows 2003 Exchange Server for Remote Operations Communication Center (ROCC), Revision 2.02*, dated January 2004, page 84.

products and periodically reviewed/audited some servers. However, the software did not continually monitor Microsoft mailbox servers for compliance with the Microsoft ES 2003 Guide, and the reviews/audits conducted provided only a snapshot result when the servers were reviewed. Failure to continuously monitor mailbox servers for compliance with security guidelines may allow the introduction of server settings that could negatively impact the operability, functionality, and security of the e-mail infrastructure.

According to SSA, the capability to meet this recommendation may be available when the Agency migrates to the Microsoft ES 2007 platform. SSA began this migration in April 2009. We therefore conclude that this recommendation has not been fully implemented.

OPEN RECOMMENDATION

Recommendation 8: Determine the feasibility of extending the e-mail retention period beyond 14 days as the Agency examines an e-mail archiving solution.

SSA agreed with this recommendation and responded as follows.

- Increasing the retention period from 14 to 30 days is feasible.
- This will require several months to implement.
- EMGB is reviewing e-mail archiving products.
- All Exchange servers will be migrated to Microsoft ES 2003 platform by April 2008.

During the current review, EMGB personnel indicated this issue will be partially addressed when the Agency migrates to the Microsoft ES 2007 server platform and fully addressed when the Agency obtains additional storage capacity. Until addressed, the Agency is at-risk that messages deleted after 14 days contain information that could be useful in fraud investigations, and Agency employee sanction activities may be permanently lost. According to SSA, this recommendation is open. We agree that this recommendation has not been implemented and remains open.

PRIOR RECOMMENDATIONS WITH WHICH SSA DID NOT AGREE

Recommendation 5: Develop, document, and test the recovery/failover capability for the e-mail messaging infrastructure, including both internal and external e-mail communications.

The Agency disagreed with this recommendation and responded that e-mail is tested in the annual disaster recovery exercise (DRE) as part of the EWAN. While our current review found SSA tested elements of e-mail as part of the FY 2008 DRE and as part of a 2007 monthly DRE conducted for the ROCCs, the testing did not include external e-mail communications. As a result, SSA still cannot ensure the continuity of operations with respect to e-mail. We continue to believe that the Agency's reliance on e-mail, as a critical tool to meet its mission, warrants taking the necessary precautions to ensure continued e-mail communications. Therefore, we reaffirm our original recommendation that SSA develop, document, and test the recovery/failover capability for the electronic messaging infrastructure to include external as well as internal e-mail communications. According to Agency personnel, this recommendation will be addressed when the co-processing center becomes operational.

Recommendation 6: Ensure appropriate risk assessments are performed on the entire e-mail system comprised of SSA's Microsoft ES 2003 environment, the OWA system and the e-mail security structure.

SSA disagreed with this recommendation and commented that e-mail and OWA reside on the EWAN platform, and the 2006 EWAN risk assessment sufficiently addressed this issue. According to Office of Management and Budget (OMB) Circular A-130, Appendix III, agencies are required to review the security controls in each system when significant modifications are made to the system.[7] Further, the security control review should be conducted using a risk assessment methodology.[8] SSA's e-mail system migrated to the Microsoft ES 2003 platform in March 2008. In addition, the SSA e-mail system has begun migration to the Microsoft ES 2007 platform with full migration planned in FY 2010. Since e-mail has not undergone a risk-based review to determine the impact these migrations will have on the e-mail infrastructure, SSA cannot ensure all risks have been identified and the system is secure. Therefore, we reaffirm our original recommendation that SSA ensure appropriate risk assessments are performed on the entire e-mail system comprised of SSA's Microsoft ES 2003 and 2007 platforms, the OWA system, and the e-mail security structure. According to Agency personnel, SSA plans to conduct a risk assessment of the entire e-mail system in FY 2010.

---

[7] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources,* section A.3.a.3, *Review of Security Controls*, states, in part, "Review the security controls in each system when significant modifications are made to the system, but at least every three years."

[8] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002, Chapter 3, Risk Assessment.

CONCLUSION AND RECOMMENDATIONS

Our initial review contained nine recommendations, of which the Agency agreed with seven. For these seven recommendations, we determined four were fully implemented, two were not fully implemented and one was not addressed.

We encourage SSA to continue its efforts to take corrective action on Recommendation 8 from our original report. We believe the implementation of a long-term e-mail archiving solution has become even more crucial. Current events demonstrate the potential significant impact that e-mail could play, in the form of evidence, or as an official document, in investigative and employee sanction activities. The *E-Government Act*[9] and NIST SP 800-45[10] collectively indicate that an effective and efficient e-mail security management program includes ensuring confidentiality, availability, and integrity of information system resources. Such a program is predicated on the development, maintenance, and implementation of policies and procedures with continuous monitoring to ensure their compliance. Implementing these recommendations would help ensure that SSA has standards and guidelines to further strengthen the infrastructure SSA has established for a sound e-mail security management program.

Because we found additional noncompliant configuration settings and an existing employee's inappropriately administered e-mail account, we are making two new recommendations that SSA:

1. Ensure e-mail server settings are configured correctly in accordance with NIST recommended standards.

2. Ensure the policies and procedures require compliance with least-privilege administrative access and appropriate chain of command approvals for e-mail account assignment.

---

[9] The E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301(b)(1), Information Security Sec. 3541: states in part that "…The purposes of this subchapter are to-- (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources," and Sec. 3542(b)(1) defines 'information security' as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity…; (B) confidentiality…; and (C) availability..."

[10] NIST SP 800-45, version 2, *Guidelines on Electronic Mail Security,* Chapter 4, sub-section 4.3 states in part that "Appropriate management practices are critical to operating and maintaining a secure mail server. "Security practices entail the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability of information system resources."

Because the Agency closed two recommendations that we believe have not been implemented, we recommend that SSA:

3. Develop and document an SSA Microsoft Exchange Server Configuration Guide[11] for e-mail settings in accordance with NIST recommended standards.

4. Continually monitor servers for compliance with SSA's Microsoft Exchange Server Configuration Guide.

With respect to the two original recommendations with which SSA disagreed, we reaffirm our recommendations that SSA:

5. Develop, document, and test the recovery/failover capability for the e-mail messaging infrastructure, to include external as well as internal e-mail communications.

6. Ensure appropriate risk assessments are performed on the entire e-mail system comprised of SSA's Microsoft ES 2003 and 2007 environments, the OWA system, and the e-mail security structure.

AGENCY COMMENTS

SSA agreed with our recommendations. The Agency's comments are included in Appendix C.

Patrick P. O'Carroll, Jr.

[11] SSA servers will operate in a 'mixed mode' environment, including both 2003 and 2007 platform servers. It is necessary that guides for both platforms be developed and used until such a time as only 2007 servers exist.

Appendices

Acronyms

CIS	Center for Internet Security
DRE	Disaster Recovery Exercise
e-mail	Electronic mail
EMGB	Electronic Messaging and Groupware Branch
ES	Exchange Server
EWAN	Enterprise Wide Mainframe and Distributed Network Telecommunications Services System
FY	Fiscal Year
ISSH	Information Systems Security Handbook
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OWA	Outlook Web Access
ROCC	Remote Operations Communication Center
SP	Special Publication
SSA	Social Security Administration

Scope and Methodology

Our objective was to determine the extent to which the Social Security Administration (SSA) implemented the recommendations in our September 2006 report, *The Social Security Administration's Electronic Mail Security Review*.

To meet our objectives, we

- documented and examined the prior report and various audit work papers;
- interviewed SSA personnel involved with addressing the prior recommendations;
- documented and examined evidence of the status of all prior recommendations; and
- examined various SSA policies regarding the use of its electronic mail system.

In addition, we reviewed 95 configuration settings on each of the 17 Microsoft Exchange Server 2003 mailbox servers tested. We reviewed two servers from each of the six Regional Operations Control Centers (Birmingham, Chicago, Kansas City, New York, Philadelphia, and San Francisco) and Headquarters. We also reviewed the Office of the Inspector General mailbox server and two servers that contained incorrect configuration settings from the prior review.

We examined these servers for compliance with Federal standards and guidelines contained in the National Institute of Standards and Technology (NIST) Special Publication 800-70.[1] The NIST program is in cooperation with checklist development activities at the Defense Information Systems Agency, the National Security Agency, and the Center for Internet Security.

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. We conducted our field work at SSA Headquarters in Baltimore, Maryland, from October 2008 through February 2009. The audited entities were the Office of System's Electronic Messaging and Groupware Branch, and the Office of Policy.

[1] NIST Special Publication 800-70, *Security Configuration Checklists Program for Information Technology (IT) Products,* May 26, 2005.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: May 26, 2009 Refer To: S1J-3

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

From: James A. Winn /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "Follow-up: The Social Security Administration's Electronic Mail Security Review" (A-14-09-19044)--INFORMATION

Thank you for the opportunity to review and comment on the draft report. We appreciate the comprehensive work that the OIG auditing team did on this report. Our response to the report findings and recommendations is attached.

Please let me know if we can be of further assistance. Please direct staff inquiries to Candace Skurnik, Director, Audit Management and Liaison Staff, at (410) 965-4636.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "FOLLOW-UP: THE SOCIAL SECURITY ADMINISTRATION'S ELECTRONIC MAIL SECURITY REVIEW" (A-14-09-19044)

Recommendation 1

Correctly configure e-mail server settings in accordance with the National Institute of Standards and Technology (NIST) recommended standards.

Comment

We agree. The audit process is on-going and we continue to move forward. We have an internal audit process in place for all existing Exchange servers. Thus, we can meet the suggested 2-year requirement.

Recommendation 2

Ensure the policies and procedures require compliance with least-privilege administrative access and appropriate chain of command approvals for e-mail account assignment.

Comment

We agree. We are accomplishing this with our existing Exchange infrastructure. We have updated our current procedures to ensure we correctly assign all Exchange mailboxes to the accurate Active Directory accounts. In anticipating the upcoming infrastructural changes in Exchange at the server and client levels, including the hardware refresh and the anticipated VISSA image, we anticipate meeting this particular requirement within the next 2 years.

Recommendation 3

Develop and document a Social Security Administration (SSA) Microsoft Exchange Server Configuration Guide for e-mail settings in accordance with NIST recommended standards.

Comment

We agree. We are currently creating new build documentation for Exchange 2007 environment. We will address NIST guidelines where essential. In anticipation of the upcoming hardware refresh, infrastructural changes in Exchange, and Outlook and the anticipated VISSA image, we foresee meeting this particular requirement within next 2 years, provided we meet all the dependencies.

Recommendation 4

Continually monitor servers for compliance with SSA's Microsoft Exchange Server Configuration Guide.

Comment

We agree. We are already accomplishing this with our current infrastructure. With the upcoming new Exchange configuration on new 64-bit hardware, we expect to meet this requirement within the next 2 years.

Recommendation 5

Develop, document, and test the recovery/failover capability for the e-mail messaging infrastructure, to include external as well as internal e-mail communications.

Comment

We agree. The Durham Support Center (DSC) will mitigate this recommendation, as there will be redundant Internet and e-mail services available from both the National Computer Center and the DSC. We look forward to establishing failover for Internal and Internet mail delivery once the Exchange servers and internet mail-hubs are completely installed and functional at the DSC. If we meet all pre-requisites, we expect to complete this process in the year 2011.

Recommendation 6

Ensure that SSA staff appropriate risk assessments on the entire e-mail system comprised of SSA's Microsoft ES 2003 and 2007 environments, the Outlook Web Access (OWA) system and the e-mail security structure.

Comment

We agree with this recommendation. We access risks as part of the certification and accreditation (C&A) process. The e-mail and OWA reside on the Enterprise Wide Mainframe and Distributed Network Telecommunications Services System (EWAN) platform. Currently, EWAN is undergoing C&A cycle and the email infrastructure is included in that process, which includes a control testing and a risk assessment. In short, the C&A process is a review of policies, procedures, controls, and contingency planning. The outcome of the C&A process is to put together a collection of documents that describe the security posture of the systems, an evaluation of the risks, and recommendations for correcting deficiencies.

[In addition to the information listed above, SSA also provided technical comments which have been addressed, where appropriate, in this report.]

OIG Contacts and Staff Acknowledgments

OIG Contacts

Phil Rogofsky, Acting Director, Information Technology Audit Division

Mary Ellen Moyer, Acting Audit Manager

Acknowledgments

In addition to those named above:

Harold Hunter, Senior Auditor

Jan Kowalewski, Systems Analyst

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-14-09-19044.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, 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, OCCIG 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.