SOCIAL SECURITY

MEMORANDUM

Date: September 24, 2009 Refer To:

To: The Commissioner

From: Inspector General

Subject: Follow-up: The Social Security Administration's Computer Security Program Compliance (A-14-09-19048)

The attached final report presents the results of our audit. Our objective was to determine whether the Social Security Administration had implemented the recommendations in our June 2001 report, *Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations* (A-13-98-12044).

Please provide within 60 days a corrective action plan that addresses each recommendation. If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

OFFICE OF THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

FOLLOW-UP: THE SOCIAL SECURITY ADMINISTRATION'S COMPUTER SECURITY PROGRAM COMPLIANCE

September 2009 **A-14-09-19048**

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.

Executive Summary

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) had implemented the recommendations in our June 2001 report, *Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations* (A-13-98-12044).

BACKGROUND

Our 2001 audit examined whether SSA's computer security program complied with the *Computer Security Act of 1987*, the *Government Information Security Reform Act of 2000* (GISRA), and other applicable laws, regulations, and Federal guidance. Our June 2001 report stated that SSA lacked a strong framework for overall security administration, policy development, and policy implementation. We recommended that SSA:

1. Centralize its systems security management structure to comply with GISRA and other applicable laws.

2. Develop a more inclusive system security plan for the mainframe and distributed computing environments.

3. Implement a global e-mail and other appropriate methods for broadcasting computer incidents.

4. Develop sanctions for users who cause system disruptions or share passwords.

5. Develop a computer system security manual consistent with guidance provided by the National Institute of Standards and Technology, and incorporate in it all existing computer security policies.

RESULTS OF REVIEW

SSA considered each of the five prior recommendations to be implemented and closed. Our follow-up review determined that SSA had implemented Recommendations 2 and 4. However, SSA had not fully addressed Recommendations 1, 3 and 5. Despite SSA's efforts to address these recommendations, our current review found that:

- SSA continued to have a decentralized/fragmented information security management structure;
- the Office of the Chief Information Officer did not have sufficient delegated authority and resources to carry out its responsibilities for SSA's information security program;

- SSA had not sufficiently documented its policy and procedures to ensure all systems users receive timely notification of imminent security incidents; and
- SSA's Information Systems Security Handbook (ISSH) did not cover all security areas and contained outdated and inaccurate information.

Although SSA had complied with certain security-related requirements, there are opportunities to improve the efficiency and effectiveness of the overall program. We believe a centralized approach to security management would be in line with the current Agency initiative of adopting a more integrated and seamless approach to systems development to address the Agency's growing needs effectively and efficiently.

CONCLUSION AND RECOMMENDATIONS

SSA has taken some actions to address the five recommendations from our prior report. Two recommendations were fully implemented, and partial corrective action has been taken on the remaining three. Based on our review and the current guidance on information security, we believe a centralized information security management structure will better position the Agency to effectively manage and monitor its agency-wide information security program. As such, we reaffirm the merits of our original Recommendation 1 and recommend that SSA:

1. Centralize its security management structure to ensure a coordinated approach to its agency-wide information security program.

2. Clearly delineate roles, responsibilities, and lines of communication that report to a single management focal point.

We have also revised previous, or included new recommendations to ensure full compliance with our prior recommendations and/or to address new issues we identified during the course of this audit. We recommend SSA:

3. Ensure the Chief Information Officer (CIO) has sufficient delegated authority and resources to fulfill his security responsibilities according to applicable laws, regulations, and guidance.

4. Update its agency-wide Information Security Program Plan.

5. As appropriate, ensure written polices and procedures require notification of all Agency systems users for certain computer incidents.

6. Update the ISSH with the most current and accurate information and consider further delineating security roles and responsibilities of Agency components and security officers related to the subject matter in each chapter. SSA should include all security policies or references in the ISSH.

AGENCY COMMENTS

SSA agreed with Recommendations 4, 5, and 6, but deferred responding to Recommendations 1, 2, and 3 until the CIO has the opportunity to review the issues discussed in the report. See Appendix E for the full text of SSA's comments.

OIG RESPONSE

We encourage the Agency to move quickly to implement Recommendations 1, 2, and 3 once the CIO has the opportunity to evaluate the issues addressed in the report. The implementation of these recommendations will help ensure a more efficient and effective management of the Agency's information security program.

Table of Contents

Introduction

OBJECTIVE

Our objective was to determine whether the Social Security Administration (SSA) had implemented the recommendations in our June 2001 report, *Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations* (A-13-98-12044).

BACKGROUND

Our 2001 audit examined whether SSA's computer security program[1] complied with the *Computer Security Act of 1987* (CSA), *Government Information Security Reform Act of 2000* (GISRA), and other applicable laws, regulations, and Federal guidance. Our June 2001 report stated that SSA lacked a strong framework for overall security administration, policy development, and policy implementation. To address these findings, we recommended that SSA:

1. Centralize its systems security management structure to comply with GISRA and other applicable laws to ensure all key security components responsible for agency-wide security policy and administration report directly to the Chief Information Officer (CIO).

2. Develop a more inclusive system security plan for the mainframe and distributed computing environments according to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18.

3. Implement a global e-mail and other appropriate methods for broadcasting computer incidents. This would include automated calling process and office intercom systems.

4. Develop sanctions for users who cause system disruptions or share passwords.

5. Develop a computer system security manual consistent with guidance provided by NIST, and incorporate in it all existing computer security policies.

The Agency agreed or partially agreed with all these recommendations. Since our 2001 audit, there have been major changes and revisions in Federal laws, regulations,

[1] During the 2001 audit, the CSA contained the major criteria related to the security of sensitive information in computer systems. We used the term "computer security program" to describe the security framework and requirements. Since 2001, *GISRA* and the *Federal Information Security Management Act*, adopted the term "agency-wide information security program" that is used in this report. For the same reason, the term "computer security" has been replaced by "information security" to include both information systems and information.

and requirements for agency-wide information security programs.[2] In this review, we examined and determined whether SSA implemented our recommendations and complied with the current Federal requirements in the related areas.

CHANGES IN LAWS, REGULATIONS AND REQUIREMENTS

Since our 2001 audit, the *Federal Information Security Management Act of 2002* (FISMA) repealed the CSA,[3] and GISRA expired in November 2002. As a result, FISMA became the overall criteria for agency-wide information security programs for Federal agencies. In addition, NIST revised and issued new security guidance that Federal agencies are required to comply with under FISMA.

FISMA requires that Federal agencies develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the agency's operations and assets.[4] FISMA also requires that a Federal agency head delegate authority to the agency CIO to ensure compliance with FISMA's requirements.[5] The CIO should appoint a senior agency information security officer[6] to head an office with the mission and resources to assist in ensuring agency compliance with FISMA.[7]

In addition to specifying responsibilities of the CIO and the senior agency information officer, FISMA also requires that an agency-wide information security program include periodic risk assessments, a risk management process, security planning, periodical security evaluations, security training, a security deficiency remediation process, an incident response process, and continuity of operations.[8] See Appendix C for more details on FISMA requirements related to security management structure.

[2] See Footnote 1.

[3] Pub. L. No. 107-347, Title III, Section 305 (a).

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

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

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

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

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

Results of Review

While SSA considered the five recommendations in our 2001 audit to be implemented and closed, based on our follow-up review, we believe there are still steps that need to be taken to fully address three of our prior recommendations. Specifically, we determined that SSA implemented prior Recommendations 2 and 4 to develop (1) a more inclusive system security plan for the mainframe and distributed computing environments and (2) sanctions for users who cause systems disruptions. However, SSA had not fully addressed the prior Recommendations 1, 3, and 5 to (1) centralize its security management structure, (2) implement a global system user notification mechanism for imminent security incidents, and (3) develop a computer system security manual to incorporate all related policies. Despite the Agency's efforts to address the prior recommendations, we found the following:

- SSA continued to have a decentralized/fragmented information security management structure.
- The Office of the CIO (OCIO) did not have sufficient delegated authority and resources to carry out its responsibilities for SSA's information security program.
- SSA had not sufficiently documented its policy and procedures to ensure all systems users receive timely notification of imminent security incidents.
- SSA's Information Systems Security Handbook (ISSH) did not cover all security areas, and contained outdated and inaccurate information.

The following sections describe the status of SSA's implementation of our 2001 recommendations as well as any additional issues identified during this review. Where warranted, we made additional recommendations to assist SSA in strengthening its agency-wide information security management posture. Given the inherent importance of the information security management structure, we expanded our work beyond just assessing SSA's implementation of our prior recommendations. See Appendix B for more details on our scope and methodology.

FULLY IMPLEMENTED RECOMMENDATIONS

Prior Recommendation 2: Develop a more inclusive system security plan for the mainframe and distributed computing environments according to NIST SP 800-18.

Our 2001 review found that SSA's System Security Plan (SSP) for the Enterprise-Wide Mainframe and Distributed Network Telecommunications Services System did not fully meet Office of Management and Budget (OMB) or NIST requirements. We reported the SSP

- did not disclose vulnerabilities;
- referred to past risk assessments when no risk assessments had been performed within the prior 5 years; and
- did not include some elements as required by OMB and NIST.

As part of our Fiscal Year 2008 FISMA review,[9] the Office of the Inspector General (OIG) and its contractor reviewed the SSPs and other Certification and Accreditation (C&A) documentation[10] for the following four SSA major applications and systems:

- Enterprise-Wide Mainframe and Distributed Network Telecommunications Services System;
- Electronic Disability System;
- Integrated Client Database; and
- Earnings Records Maintenance System.

We found SSA had performed risk assessments and developed SSPs for these systems. We concluded that SSA's C&A documentation, including the risk assessments and SSPs, generally addressed all elements as recommended by OMB and NIST requirements. As a result, we consider this recommendation implemented.

Prior Recommendation 4: Develop sanctions for users who cause system disruptions or share passwords.

Our 2001 review reported that while SSA's security program described sanctions for unauthorized systems access, it did not document sanctions for users who disrupt system operations, cause systems to shutdown, or share passwords. SSA originally agreed with the recommendation but after further review of its policies, determined that a separate set of sanctions did not need to be developed to implement this recommendation.

---

[9] SSA OIG, *Fiscal Year 2008 Evaluation of the Social Security Administration's Compliance with the Federal Information Security Management Ac* (A-14-08-18063), September 2008.

[10] C&A is the authorizing process for the use of information systems. SSA's C&A documentation for a major application or system includes a System Security Plan, Risk Assessment Report, and Security Control Assessment Report.

SSA's *Rules of Behavior for Users and Managers of SSA's Automated Information Resources* describe expected behavior for all SSA personnel, contractors, and external users of SSA's information systems. It states, "Failure to follow these prescribed rules, and/or misuse of information resources, can lead to suspension, termination or other administrative or legal actions based on the seriousness of the violation." As a result, we concluded that SSA had addressed the intent of this recommendation.

PARTIALLY IMPLEMENTED RECOMMENDATIONS

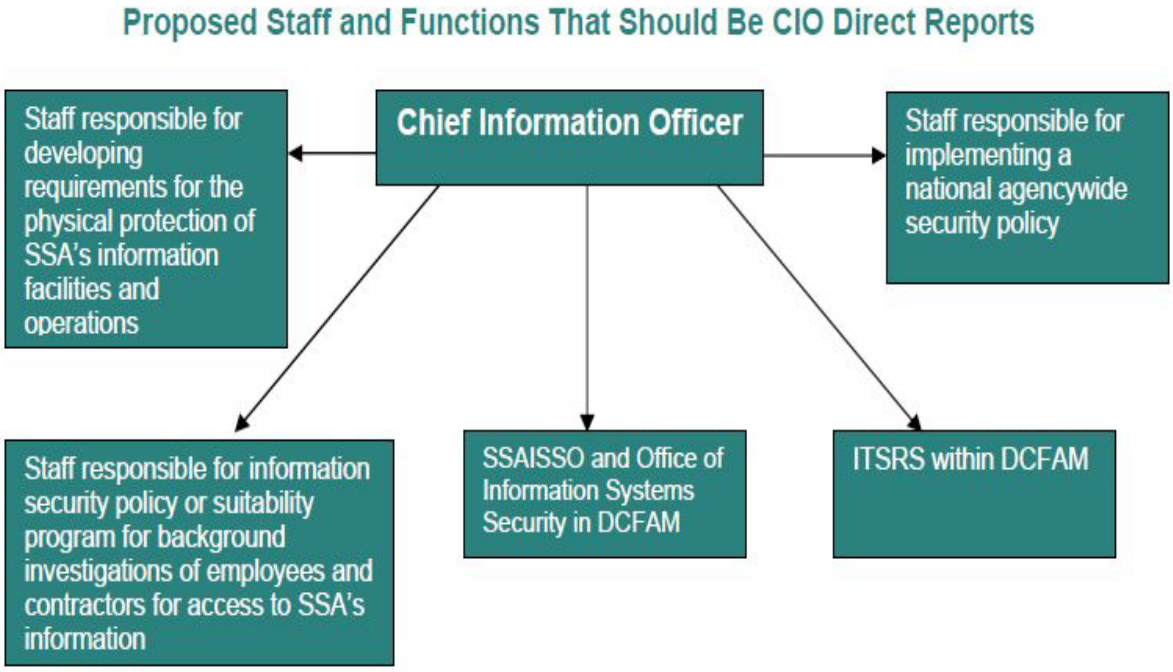
Prior Recommendation 1: Centralize the systems security management structure to comply with GISRA and other applicable laws to ensure that all key security components responsible for agencywide security policy and administration report directly to the CIO.

In our 2001 review, we found the security and information technology (IT) management components under various Deputy Commissioner (DC) offices did not directly report to the CIO.

We provided the following diagram to SSA as an example of the proposed staff and functions that we recommended as direct reports to the OCIO. It should be noted that some of the acronyms for components that existed when we issued the 2001 report have now been re-titled. Please see the footnote below.[11]

[11] The diagram is documented in our 2001 report, page 7. Information Technology Systems Review Staff (ITSRS) was re-titled the Office of Information Technology Investment Management. The Deputy Commissioner for Finance, Assessment, and Management (DCFAM) has been re-titled the Deputy Commissioner for Budget, Finance and Management. SSA Information Systems Security Officer (SSAISSO) was responsible for developing agency-wide information security policies and procedures and ensuring proper implementation of the policies. SSA's Chief Information Security Officer resumed the policy-making responsibilities of the prior SSAISSO. The Office of Information Systems Security was re-titled the Office of Information Technology Security Policy.

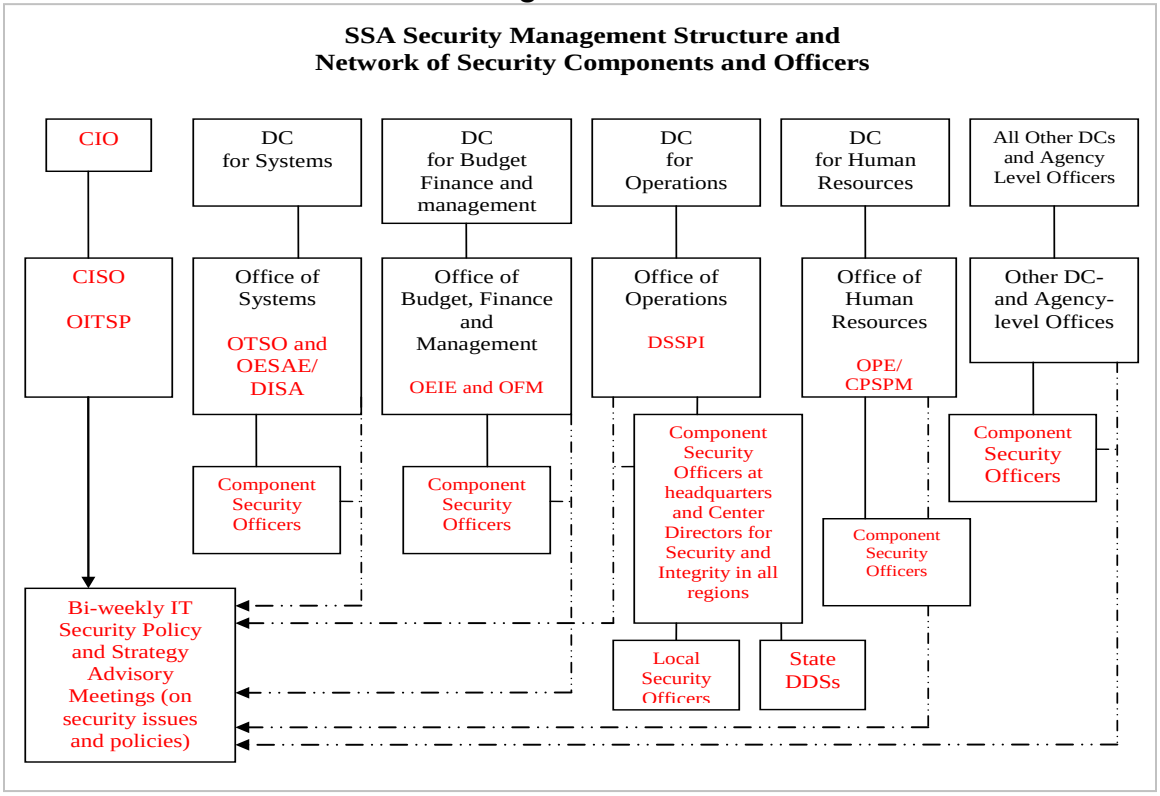
Diagram 1



The Agency agreed in principle with the recommendation but did not agree to move all functions that we recommended under the direct supervision of the CIO. Instead, SSA responded that it would review the capacity of the OCIO to directly oversee computer security and asset management functions.

Since our 2001 audit, SSA moved the CIO from the immediate Office of the Commissioner and created the new OCIO. The OCIO was established as an Agency-level office whose head is appointed by the President or by the Commissioner, if delegated by the President, for a 6-year period. At the same time, SSA abolished the Information Technology Systems Review Staff and the Office of Information Systems Security in DCFAM and transferred the policy functions of both to the OCIO. In addition, SSA established two major offices that report directly to the CIO—the Office of Information Technology Investment Management (OITIM) and the Office of Information Technology Security Policy (OITSP). OITIM is responsible for SSA's information technology (IT) capital investment planning and investment control process. OITSP establishes agency-wide security policies and manages the reporting and evaluation processes for SSA's FISMA compliance. SSA also established the position of the Chief Information Security Officer (CISO) to head OITSP. See the following diagram for the current information security management structure (see a detailed description of the diagram in Appendix D).

Diagram 2[12]



In the diagram above, the offices depicted in red perform some aspect of information security management. Because SSA did not fully address the recommendation to centralize its information security management structure, it continues to have a decentralized/fragmented information security management structure without a single management focal point. Furthermore, we determined the OCIO does not have sufficient delegated authority. As detailed in the section on *SSA's Decentralized Security Program Structure Lacks a Single Management Focal Point*, we illustrate the decentralized roles and responsibilities that yield a stove-piped approach to security with limited communication.

The Chairman of the Social Security Advisory Board, in recent testimony before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives,[13] suggested that the recently identified issues with SSA's processing

[12] For additional acronyms in Diagram 2: OTSO, Office of Telecommunications and Systems Operations; OESAE/DISA, Office of Enterprise Support, Architecture and Engineering/Division of Information Security and Assurance; OEIE, Office of Electronic Information Exchange; OFM, Office of Facilities Management; DSSPI, Division of Systems Security and Program Integrity; OPE/CPSPM, Office of Personnel/Center for Personnel Security and Project Management; DDS, Disability Determination Services.

[13] Statement of Sylvester J. Schieber, Chairman, Social Security Advisory Board to the Subcommittee on Social Security House Committee on Ways and Means, U.S. House of Representatives, *Oversight Hearing on the Progress made by the Social Security Administration in Implementing the American Recovery and Reinvestment Act of 2009*, April 28, 2009.

center[14] are rooted in SSA's decentralized IT investment governance process, exposing SSA's system infrastructure to great risk. The Chairman stated SSA's decentralized IT governance process has resulted in a dilution of ownership and management of the Agency's overall IT process. The Board believed that it would take strong leadership for the Agency's IT governance to be more productive and ensure SSA's infrastructure is not exposed to such risk again. The Board recommended that SSA restructure its governance process and centralize overall responsibility for all IT processes.

Likewise, we believe it is critical that SSA consider a centralized security management structure that provides the CIO with sufficient delegated authority and resources to fulfill his responsibilities. Although SSA has managed to comply with certain security-related requirements, there are opportunities to improve the efficiency and effectiveness of the overall program. We believe a centralized approach to security management would be in line with the current Agency initiative of adopting a more integrated and seamless approach to systems development to address the growing needs of the Agency in an effective and efficient manner. To that end, we reaffirm our original recommendation for SSA to centralize its information security management structure.

As detailed in the section on *SSA's CIO does not have Sufficient Delegated Authority and Resources to Carry Out Required Security Monitoring and Management Responsibilities,* we discuss how resource levels impact the CIO security functions. We believe it is critical that these functions receive the resources needed to carry out security management and oversight responsibilities. The following sections describe the status of SSA's decentralized information security management structure and the need for additional resources in the CIO functions.

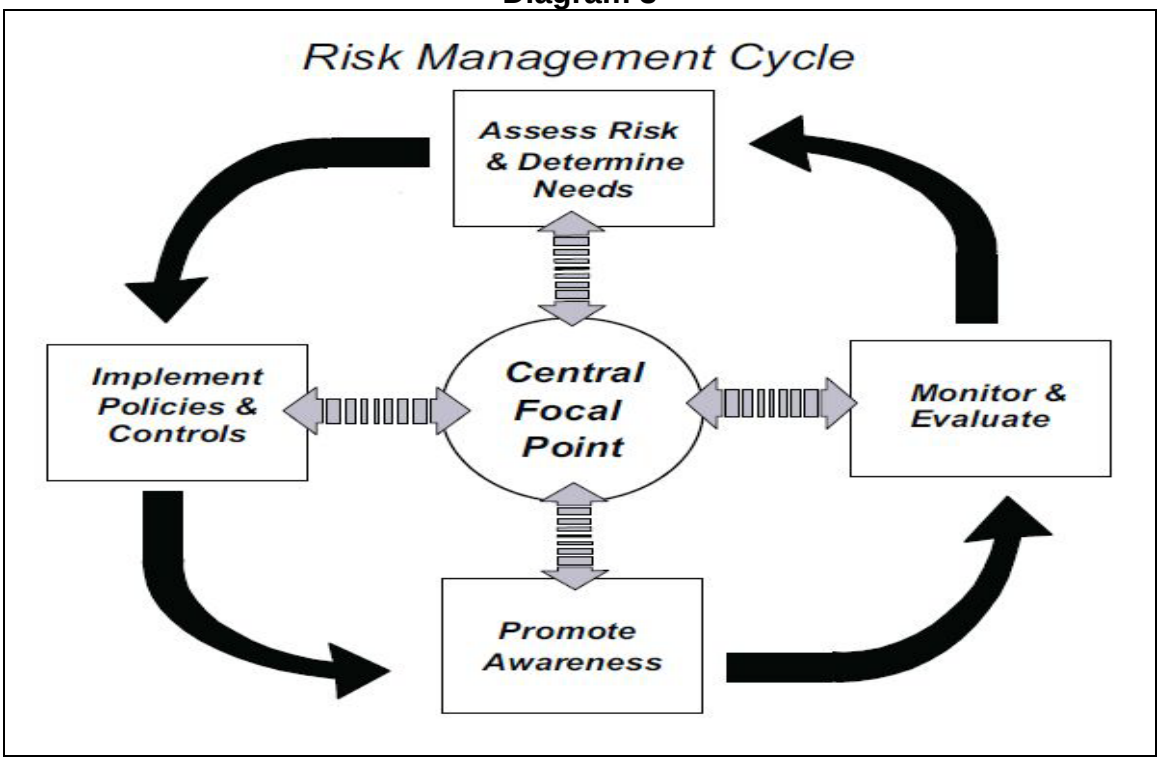
SSA's Decentralized Security Program Structure Lacks a Single Management Focal Point

A Government Accountability Office (GAO) survey of leading organizations found that a central management focal point is one of the principles embraced by all the organizations. GAO identified five risk management principles that provided a framework for an effective Information Security Program.[15]

[14] The Board stated that the current 30-year old data processing center, the National Computer Center (NCC), would no longer be viable by the end of 2012. A new NCC will take 4 to 5 years to build. However, by 2013, the second data center designed as a fully functional co-processing facility to the NCC is expected to have full backup capacity for the NCC.

[15] GAO *Executive Guide: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68, May 1998, pages 17-18.

Diagram 3



SSA's practices in information security risk management generally contain the elements identified in the model, with the exception of the central management focal point. At SSA, tasks in the risk management cycle in the above diagram are performed by different components in different DC-level offices without a central reporting structure. The following describes the key offices and officers who have security responsibilities and play significant roles in SSA's agency-wide security program.

- The Office of Electronic Information Exchange (OEIE), within the Office of Budget, Finance and Management (OBFM), is responsible for security administrative controls, security training, managing on-site system reviews, and managing and directing a comprehensive security compliance and monitoring program. OEIE develops security procedures and requirements that are followed by SSA components and security officers agencywide and is responsible for the security program for SSA's data exchange programs.
- The Office of Telecommunications and Systems Operations (OTSO), within the Office of Systems (Systems), is responsible for technical controls and requirements development, implementation, and monitoring; identifying and providing IT security incident data to the CISO for external reporting; and planning, executing, and maintaining SSA's disaster recovery program for critical information systems.
- The Division of Systems Security and Program Integrity (DSSPI), within the Office of Operations (Operations), manages a national security program with different levels of security offices and officers that cover all SSA regional offices, field offices, teleservice centers, program service centers, and all Headquarters Operations components.

- Component Security Officers are responsible for ensuring compliance with security requirements for DC-level offices and Agency-level offices.

These components and security officers form the network of SSA's security program but do not report to the CIO. In addition, some important security functions and programs managed and performed by these components and security officers do not involve the OCIO. For example, the Onsite Security Control and Audit Review program that includes systems security and physical security of many operating units, field offices, and program service centers, does not involve the OCIO. Not only is there no OCIO involvement, the results of these reviews are not shared with OCIO. The security components and security officers of the national security program, managed by Operations, that handle daily security issues and ensure security compliance do not report to the CIO. Furthermore, the security components in OTSO in charge of technical controls implementation and monitoring do not report to the CIO.

Although the OCIO is responsible for the Agency's information security program, the CIO's authority is inherently limited by the current security management structure. Under the current structure, the CIO is only responsible for security policy-making and FISMA reporting. The CIO does not oversee and monitor agency-wide compliance with FISMA and other security standards and requirements. Each DC and Agency-level office is responsible for compliance with all security requirements for their respective component but does not periodically report to the CIO. Our review found that none of the security components or offices was responsible for ensuring agency-wide security compliance. As a result, SSA's security management structure was fragmented and not as effective as it could be.

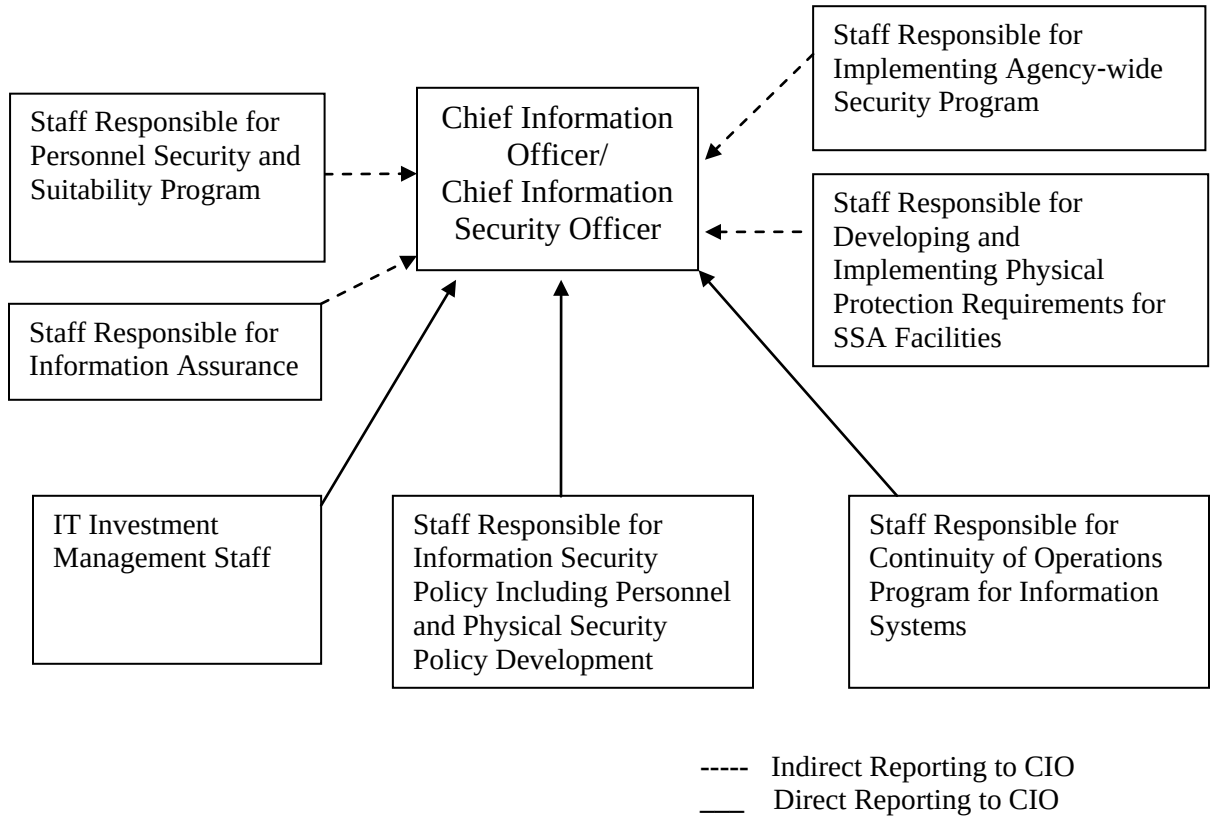
Although the CIO is, by law, responsible for ensuring agency-wide security compliance, the CIO does not have the delegated authority, resources, and staff with necessary expertise to conduct sufficient compliance monitoring activities. Even within the security functions performed by OCIO, it largely relies on other components to cooperate and provide data, resources, and expertise.

As a result, the OCIO experienced many challenges that included the following:

- Setting security policies and changes in security environment or controls is a time-consuming negotiation process that may take months to years to obtain security components' cooperation and agreement on security policies and issues.
- The OCIO does not have the capability of adequately and timely reporting to higher oversight authorities on security issues and major incidents.
- The OCIO cannot ensure an effective agency-wide security program, given the limited authority and resources.
- The OCIO does not have sufficient access to critical data, reports, and documentation to perform their duties.

To fully comply with FISMA and other applicable laws and regulations, SSA needs to have all staff responsible for developing agency-wide security policy report to the CIO. Staff responsible for administering component information security policy related to day-to-day operations and consistent with agency-wide security policy should indirectly report to the CIO through their respective DC or equivalent. We suggest the following reporting of staff and functions to the CIO.

Recommended Staff Functions and Reporting Lines



This proposed security management structure would best position SSA to implement and maintain an agency-wide security program, especially with increased public access to Social Security services via the Internet and growing systems interconnectivity. Solid lines show direct reporting to the CIO, while dotted lines show indirect reporting to the CIO through an organization's respective DC or equivalent. This diagram does not include staff responsible for network operations. For more details on the functions performed by staff in this diagram, see Appendix D.

"For a central computer security program to be effective, it should be an established part of organization management."[16] The NIST guidance states that a ". . . well established program will have a program manager recognized within the organization as the central computer security program manager."[17] "In addition, the program will be staffed with able personnel, and links will be established between the program management function and computer security personnel in other parts of the organization."[18] SSA needs to have a single authority and a driving force to ensure the effectiveness of its security program. We continue to recommend that SSA centralize its management structure to ensure the effectiveness of its security program.

SSA's CIO Does Not Have Sufficient Delegated Authority and Resources to Carry Out Required Security Monitoring and Management Responsibilities

According to FISMA, each agency is required to implement an agency-wide information security program to provide security for its information and information systems that support the operations and assets of the agency.[19] The 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.[20] Furthermore, NIST guidance states that the security program should also address compliance with national policies and requirements as well as organization-specific requirements.[21]

Although SSA has substantially complied with FISMA, SSA's CIO does not have sufficient delegated authority, resources, and expertise to fulfill all required FISMA responsibilities. The CIO's delegated authority and functions are limited to setting agency-wide security policies and FISMA-related testing, evaluation, and reporting. Except for the functions OCIO retains, all FISMA IT security program-related functions and responsibilities are delegated to OBFM, Systems, Operations, and other components. The CIO and CISO currently have a security staff of eight, supplemented with approximately six contractors. At this staffing level, some functions defined and implied by FISMA as major responsibilities of the CIO are not performed by the OCIO at SSA. For example, SSA's OCIO does not

- manage, direct, or monitor SSA's agency-wide security program as a whole;
- run an agency-wide compliance monitoring program to ensure compliance with FISMA and other security standards and requirements;

---

[16] NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995, section 6.3, page 51.

[17] Id.

[18] Id.

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

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

[21] NIST, supra, section 6.3, page 52.

- have authority over personnel security, physical security, and security of SSA's data exchange program; or
- lead SSA's Continuity of Operations program for information systems.

SSA should assess the appropriate staffing level for the OCIO commensurate with its security responsibilities, and provide sufficient resources to the OCIO so it can maintain, manage, and monitor a security program that covers about 64,000 SSA employees and 25,000 contractors. In addition, the CIO does not have the level of delegated authority commensurate with the CIOs responsibilities. For example, the security component within OBFM, OEIE, chairs SSA's Critical Infrastructure Protection Committee and serves as the representative for its entity-wide security program[22] under the annual financial statement audit. The CIO should have sufficient delegated authority, staff, and resources to implement and maintain an agency-wide compliance monitoring program and to fulfill other security management responsibilities.

Prior Recommendation 3: Implement a global e-mail and other appropriate methods for broadcasting computer incidents. This would include an automated calling process and office intercom systems.

Our 2001 review reported that during the ***"I LOVE YOU"*** virus attack, SSA was unable to immediately inform all SSA employees of the attack and had to temporarily shut down Agency e-mail systems to prevent the spread of the virus. While SSA agreed with, and had taken steps to, implement our recommendation, we concluded that SSA had not fully implemented this recommendation.

SSA stated it uses a broadcasting tool as well as global e-mail messages to inform employees of outages, system updates, and security incidents. However, we found that SSA has not sufficiently documented these procedures in the ISSH and related incident handling and reporting guide.

We recommend that SSA properly document the incident broadcasting process so the policy and procedures are readily available for all SSA users, and that all SSA systems users are timely and properly informed when certain computer incidents occur.

Prior Recommendation 5: Develop a computer system security manual consistent with guidance provided by NIST and incorporate in it all existing computer security policies.

In our 2001 report, we found SSA did not have all security policies and procedures integrated into one comprehensive document. SSA agreed with the recommendation and has made improvements. Since our 2001 review, SSA further integrated security policy into its ISSH by including electronic links and references to SSA management and operations manuals and Federal laws, regulations, and guidance. However ISSH

[22] The GAO *Federal Information System Controls Audit Manual* uses the term entity-wide security program rather than agency-wide security program.

does not include all security-related policies. For example, ISSH does not include SSA's security policy or references related to its State data exchange programs, State Disability Determination Services, and physical and facility protection. ISSH is also not clear about SSA's policy on timely informing all employees and systems users about malicious security incidents. We concluded that SSA had not fully addressed our recommendation.

While conducting this review, we identified the following areas where SSA can further improve its current ISSH and security program documentation:

1. SSA Should Update its Agency-Wide Information Security Program Plan

SSA has referred to the ISSH as its documented agency-wide security program. However, ISSH does not include an agency-wide master plan that documents how SSA protects its information and information systems. SSA's OCIO had posted an *IT Systems Security Plan* on the OITSP website. However, this document had not been updated to reflect SSA's current agency-wide security program plan.

SSA should have a written plan that clearly describes its information security program in addition to the policies and procedures that support the program. During this review, we found the OCIO is drafting an IT Security Program Plan.

2. Roles and Responsibilities are not Defined Clearly in the ISSH Chapters

Each chapter of the ISSH has a section called *Roles and Responsibilities* that lists components, security officers, managers, and users who have specific responsibilities for the subject matter of the chapter through electronic links to general descriptions of their security roles and responsibilities. However, ISSH did not clearly delineate their roles and responsibilities directly related to the chapter. For example, the chapter on Systems Access Policy lists OITSP as one of the components that has specific responsibilities by providing an electronic reference link; however, it does not link to a description of specific access control responsibilities for OITSP.

Federal guidance requires that security responsibilities be clearly delineated and specifically assigned to the organization elements and officials responsible for the implementation and continuity of the computer security policy.[23] SSA needs to provide a more specific description of what responsibilities the security components and officers have in the security areas discussed in each ISSH chapter.

3. ISSH Needs to be Revised and Updated with the Most Current and Accurate Information

- The Security Organizational Structure diagram documented in Chapter 1 does not reflect the current authority structure of SSA's security management program. For example, the Center Directors for Integrity and Security report to the Assistant

[23] NIST, supra, section 5.1.1, page 36.

Regional Commissioners in Operations. However, the ISSH diagram indicates they report to OEIE in OBFM. Further, none of the security components directly report to the OCIO, as indicated in the diagram.

- The ISSH contains old component names, outdated guidance, and duplicate information.

SSA should review the current ISSH to ensure it contains the most current and accurate information.

Conclusion and Recommendations

SSA has taken some actions to address the five recommendations from our 2001 report. Two recommendations were fully implemented and partial corrective action has been taken on the remaining three. Based on our review of the current guidance on information security, we believe a centralized information security management structure will better position the Agency to effectively manage and monitor its agency-wide information security program. As such, we reaffirm the merits of our previous Recommendation 1 and recommend that SSA:

1. Centralize its security management structure to ensure a coordinated approach to its agency-wide information security program.
2. Clearly delineate roles, responsibilities, and lines of communication that report to a single management focal point.

We have also revised previous, or included new recommendations to ensure full compliance with our prior recommendation and/or to address new issues we identified during this audit, as set forth below.

3. Ensure the CIO has sufficient delegated authority and resources to fulfill required security responsibilities according to applicable laws, regulations, and guidance.
4. Update the agency-wide Information Security Program Plan.
5. As appropriate, ensure written polices and procedures require notification of all Agency systems users for certain computer incidents.
6. Update the ISSH with the most current and accurate information, and consider further delineating security roles and responsibilities of Agency components and security officers related to the subject matter in each chapter. SSA should include all security policies or references in the ISSH.

AGENCY COMMENTS

SSA agreed with Recommendations 4, 5, and 6, but deferred responding to Recommendations 1, 2, and 3 until the CIO has the opportunity to review the issues discussed in the report. See Appendix E for the full text of SSA's comments.

OIG RESPONSE

We encourage the Agency to move quickly to implement Recommendations 1, 2, and 3 once the CIO has the opportunity to evaluate the issues addressed in the report. The implementation of these recommendations will help ensure a more efficient and effective management of the Agency's information security program.

Appendices

Acronyms

C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPSPM	Center for Personnel Security and Project Management
CSA	*Computer Security Act of 1987*
CSI	Center for Security and Integrity
CSO	Component Security Officer
DC	Deputy Commissioner
DCFAM	Deputy Commissioner for Finance, Assessment and Management
DDS	Disability Determination Services
DISA	Division of Information Security and Assurance
DSSPI	Division of Systems Security and Program Integrity
FISMA	*Federal Information Security Management Act of 2002*
GAO	Government Accountability Office
GISRA	*Government Information Security Reform Act of 2000*
ISSH	Information Systems Security Handbook
IT	Information Technology
ITSRS	Information Technology Systems Review Staff
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OBFM	Office of Budget, Finance and Management
OCIO	Office of the Chief Information Officer
ODD	Office of Disability Determinations
OEIE	Office of Electronic Information Exchange
OESAE	Office of Enterprise Support, Architecture and Engineering
OFM	Office of Facilities Management
OIG	Office of the Inspector General
OITIM	Office of Information Technology Investment Management
OITSP	Office of Information Technology Security Policy
OMB	Office of Management and Budget
OPE	Office of Personnel

Operations	Office of Operations
OTSO	Office of Telecommunications and Systems Operations
Pub. L. No.	Public Law Number
SP	Special Publication
SSA	Social Security Administration
SSAISSO	SSA Information Systems Security Officer
SSP	System Security Plan
Systems	Office of Systems
U.S.C.	United States Code

Scope and Methodology

Our objective was to determine whether the Social Security Administration (SSA) implemented the recommendations in our June 2001 report, *Compliance of the Social Security Administration's Computer Security Program with Applicable Laws and Regulations* (A-13-98-12044).

The applicable laws for agency-wide information security programs have changed since our 2001 audit. Our current audit was conducted according to the security framework and requirements established by and according to the *Federal Information Security Management Act of 2002* and related Federal guidance.

We examined the prior report; compared the criteria used in the prior audit with current criteria; interviewed SSA personnel currently responsible for addressing the prior recommendations; and reviewed and examined SSA documentation for implementing our recommendations and related policy and procedures against Federal criteria.

We reviewed the following criteria:

- *Computer Security Act of 1987*;
- *Government Information Security Reform Act of 2000*;
- *Federal Information Security Management Act of 2002*;
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*,11/28/2000, Appendix III, *Security of Federal Automated Information Resources*;
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Revision 1, February 2006;
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2, December 2007;
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995;
- NIST SP 800-61, *Computer Security Incident Handling Guide*, Revision 1, March 2008; and
- Government Accountability Office, *Executive Guide: Information Security Management, Learning from Leading Organizations*, GAO/AIMD-98-68, May 1998.

We contacted or interviewed SSA staff from the following components, or reviewed the contents of their websites related to their security functions and security documents:

- SSA Chief Information Security Officer;

- Office of the Chief Information Officer (OCIO), Office of Information Technology Security Policy;
- Office of Budget, Finance and Management, Office of Strategic Services, Office of Electronic Information Exchange (OEIE);
- Office of Operations, Office of Public Service and Operations Support, Division of Systems Security and Program Integrity; and
- Office of Systems, Office of Telecommunications and Systems Operations, Division of Information Systems Security Administration and Operations.

We reviewed the following SSA documents:

- *Information Systems Security Handbook*;
- *Rules of Behavior for Users and Managers of SSA's Automated Information Resources*, March 23, 2001;
- SSA Memorandum, *Sanctions for Unauthorized Systems Access Violations and Guidance for Employees on How to Transact Social Security Business that Requires System Access*, May 15, 2008;
- OCIO, *Social Security Administration Information Technology Security Policy and Standards Development and Issuance Process*, August 14 2008;
- OCIO, *Social Security Administration Computer Security Incident Reporting Process,* August 14, 2008;
- *IT Systems Security Plan*;
- OEIE, *Information Security Officer Guide*, Revised November 2008; and
- Onsite Security Control and Audit Review guides, chapters related to systems and physical security.

We conducted this 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 December 2008 through May 2009.

Federal Information Security Management Act Requirements Related to Security Management Structure

SECURITY OFFICERS' ROLES AND RESPONSIBILITIES BY CURRENT LAW

The *Federal Information Security Management Act of 2002* (FISMA) requires that a Federal agency head delegate to the agency Chief Information Officer (CIO) the authority to ensure compliance with FISMA requirements.[1] The agency CIO has the following responsibilities:[2]

1. designating a senior agency information security officer;
2. developing and maintaining an agency-wide information security program;
3. developing and maintaining information security policies, procedures and control techniques to address all applicable requirements;
4. training and overseeing personnel with significant responsibilities for information security;
5. assisting senior agency officials concerning their responsibilities in providing information security for the information and information systems that support the operations and assets under their control (including through risk assessments, assessment of levels of security necessary, cost-effective measures to reduce risk to acceptable levels, and periodic testing and evaluating security controls and techniques to ensure they are effectively implemented);[3] and
6. reporting annually to the agency head on the effectiveness of the agency's information security program.[4]

The senior agency information security officer should head an office with the mission and resources to assist in ensuring agency compliance with FISMA.[5]

---

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

[2] Id.

[3] Pub. L. No. 107-347, Title III, Section 301 (b)(1) § 3544 (a)(2) and (a)(3)(E), 44 U.S.C. § 3544 (a)(2) and (a)(3)(E).

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

[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).

FISMA DEFINITION OF AGENCY-WIDE INFORMATION SECURITY PROGRAM

In addition to specifying responsibilities of the CIO and senior agency information officer, FISMA also defines what an agency-wide information security program should include.[6]

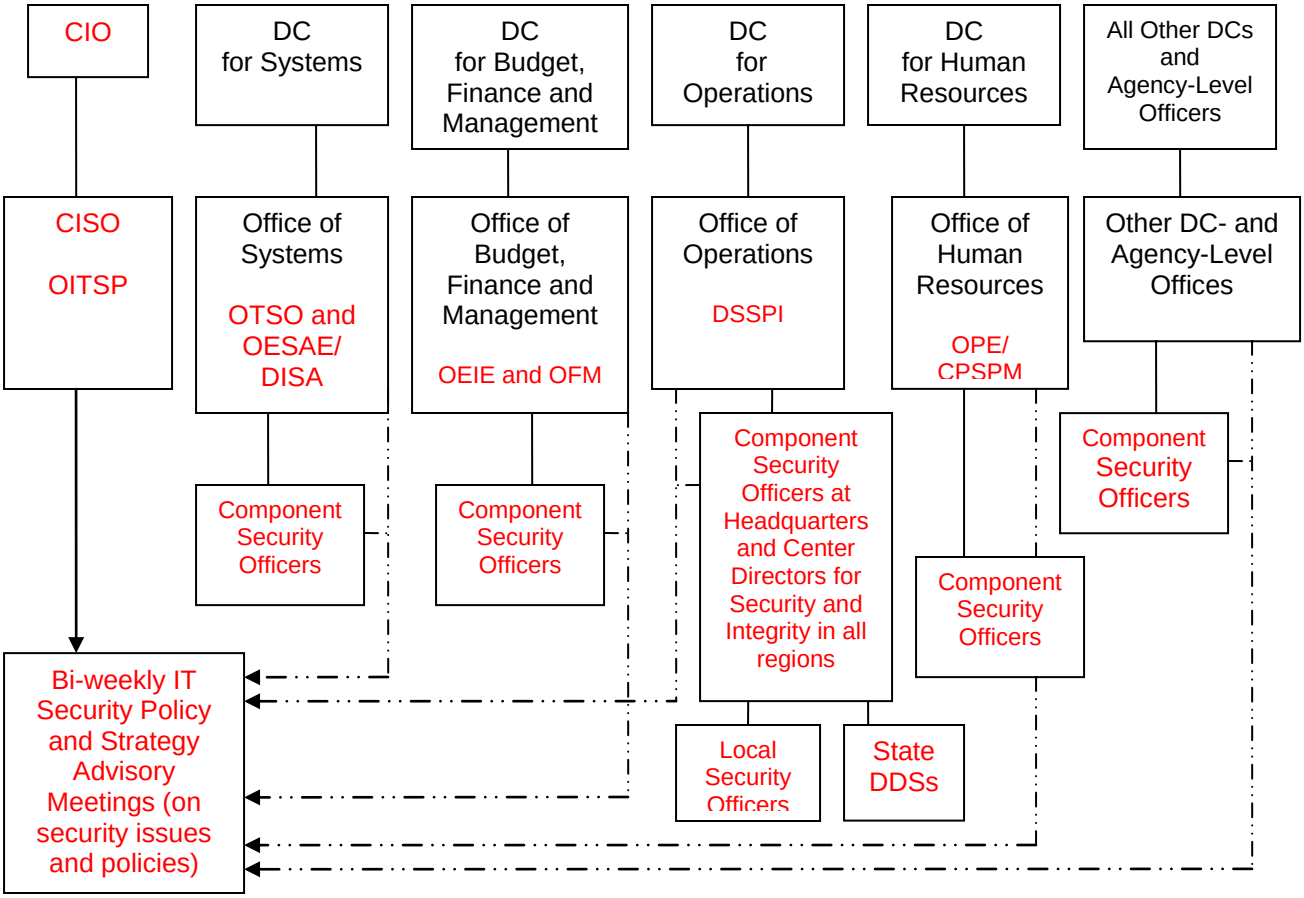
1. Periodic risk assessments;
2. Policies and procedures that: are based on a risk assessment, are cost effective in reducing risk, and ensure information security is addressed through the life cycle of each agency information system and compliance with applicable security requirements;
3. Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
4. Security awareness training for employees and contractors and other users of information systems;
5. Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (at least annually);
6. A process for remedial actions to address security deficiencies in the information security policies, procedures, and practices of the agency;
7. Procedures for detecting, reporting, and responding to security incidents; and
8. Plans and procedures to ensure continuity of operations for information systems.

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

Current Social Security Administration Security Management Structure and the Office of the Inspector General Recommended Staff Functions and Reporting Lines

The Social Security Administration's (SSA) agency-wide security program is highly decentralized with security responsibilities and functions conducted by several security components and a network of security officers. None of the security components or security officers is responsible for ensuring agency-wide compliance with the Federal security requirements. Each Deputy Commissioner-level and Agency-level office is responsible for its own compliance with all security requirements. The security components and security officers report to their respective Deputy Commissioners (DC) and Agency-level officers, who do not report to the Chief Information Officer (CIO) for security compliance and performance. See the following diagram for an overall management structure of SSA's security program.

SSA Security Management Structure and Network of Security Components and Officers



Office of the CIO, Office of Information Technology Security Policy (OITSP) headed by SSA's Chief Information Security Officer (CISO) - In supporting the CIO, the CISO and the OITSP are responsible for issuing security policies and *Federal Information Security Management Act of 2002* related testing, evaluation, and reporting. Except for functions retained by CISO and OITSP, SSA delegates all remaining security program functions to other components. In other functional areas within SSA's security program, the CISO does not have authority and, for the most part, acts in a coordinating and supporting role. OITSP conducts limited monitoring activities through bi-weekly meetings with security components to discuss security issues and policies.

Office of Budget, Finance and Management (OBFM), Office of Electronic Information Exchange (OEIE) - Formerly known as the Office of Systems Security Operations Management, OEIE plays an important role in SSA's agency-wide security program. OEIE's agency-wide security responsibilities include: development of SSA's security program requirements and procedures; implementation of governing directives in the area of systems security; administration of the Agency's access control program;

management of an onsite systems review program and a comprehensive security compliance and monitoring program; and providing direction to the Agency's security officers.

OEIE is also responsible for maintaining security policy documentation, providing security training, implementing security requirements, and executing safeguards for SSA's State information exchange programs. OEIE chairs SSA's Critical Infrastructure Protection Committee and serves as the Agency representative for its entity-wide security program for the annual financial statement audit. However, OEIE does not have the responsibility to ensure security controls are implemented and enforced agency-wide.

OBFM, Office of Facilities Management (OFM) - OFM directs SSA's physical and protective security program and establishes policy to ensure the safety and security of SSA employees, visitors, and property.

Office of Operations (Operations), the Division of Systems Security and Program Integrity (DSSPI) - DSSPI along with the regional Centers for Security and Integrity (CSI) are responsible for developing, coordinating, and implementing a comprehensive national program for Operations to focus on systems security and programmatic fraud issues. This program covers all components within Operations including regional offices, program service centers, teleservice centers, field offices, and all Operations Headquarters components. DSSPI and CSIs work with Local Security Officers at the field office level regarding security issues.

Office of Systems (Systems), Office of Telecommunications and Systems Operations (OTSO) - OTSO is responsible for implementing technical security controls and procedures and SSA's Disaster Recovery planning, testing, and execution. OTSO also monitors security controls and configurations for compliance and maintains the information system for cyber security incident identification and reporting. However, OTSO does not have agency-wide responsibility to ensure technical security compliance.

Systems, Office of Enterprise Support, Architecture and Engineering (OESAE), the Division of Information Security and Assurance (DISA) - Within Systems, provides comprehensive security services, solutions, and best practices that enhance information assurance and security for software applications assuring they are efficient, secure, and compliant with Agency and Federal information system security requirements.

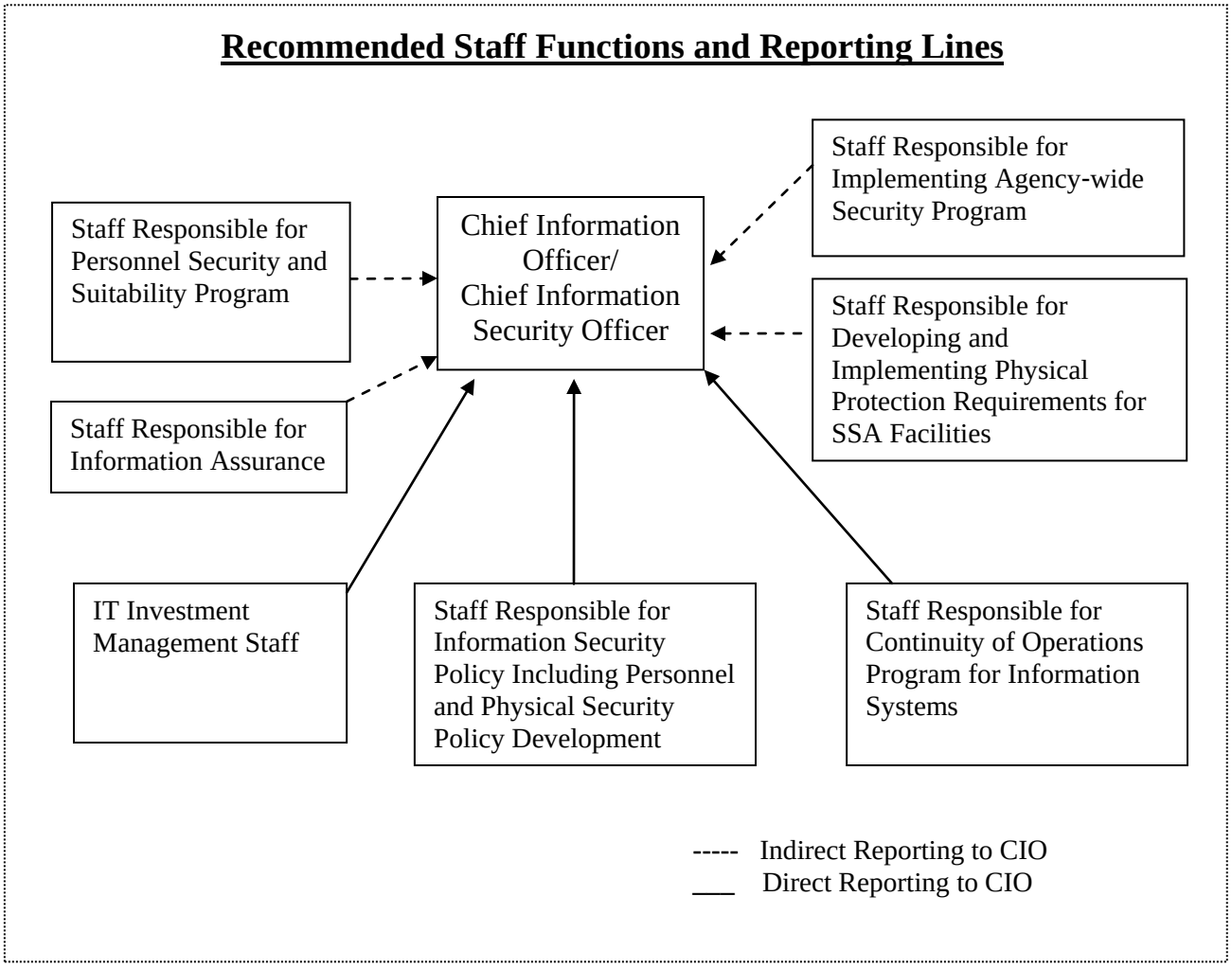
Office of Human Resources, Office of Personnel (OPE), the Center for Personnel Security and Project Management (CPSPM) - CPSPM manages SSA's nationwide programs for personnel security and suitability and national security for employees and contractors. CPSPM is also responsible for policy development in the area.

Component Security Officers (CSO) - Within SSA Headquarters, including all DC-level and Agency-level offices, CSOs are responsible for ensuring compliance within their respective components.

Office of Disability Determinations (ODD) - Within Operations, ODD coordinates and distributes regulations and policy to the State Disability Determination Services (DDS). DDS management has overall responsibility for the security of their site and compliance with established security policies and procedures. DDS management is also responsible for notifying and reporting any security breach or incident to SSA offices within the region.

RECOMMENDED STAFF FUNCTIONS AND REPORTING LINES

We recommended the following staff functions and reporting lines:



- Staff Responsible for Implementing Agency-wide Security Program: DSSPI staff within Operations and OTSO staff within Systems need to indirectly report to the CIO.

- Staff Responsible for Developing and Implementing Physical Protection Requirements for SSA Facilities: The facility management staff within OBFM need to indirectly report to the CIO.

- Staff Responsible for Continuity of Operations Program for Information Systems: OTSO Disaster Recovery staff need to directly report to the CIO.

- Staff Responsible for Information Security Policy Including Personnel and Physical Security Policy Development: Current OCIO staff and any other staff responsible for personnel and physical security policy development need to directly report to the CIO.

- IT Investment Management Staff: These staff currently report to the CIO.

- Staff Responsible for Information Assurance: DISA staff within Systems need to indirectly report to the CIO.

- Staff Responsible for Personnel Security and Suitability Program: The Center for Personnel Security and Project Management staff within the Office of Human Resources need to indirectly report to the CIO.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: September 9, 2009 Refer To: S1J-3

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

From: Margaret J. Tittel /s/
Acting Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "Follow-Up: The Social Security Administration's Computer Security Program Compliance" (A-14-09-19048)--INFORMATION

Thank you for the opportunity to review and comment on the draft report. We appreciate OIG's efforts in conducting this review. Attached is our response to the report recommendations.

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 (OIG) DRAFT REPORT, "FOLLOW-UP: THE SOCIAL SECURITY ADMINISTRATION'S COMPUTER SECURITY PROGRAM COMPLIANCE" (A-14-09-19048)

Recommendation 1

SSA should centralize its security management structure to ensure a coordinated approach to its agency-wide information security program.

Comment

We defer comment until our new Chief Information Officer (CIO) has the opportunity to review the issue of a centralized security management structure. We also plan to convene a workgroup to review any underlying issues and make recommendations as appropriate.

Recommendation 2

Clearly delineate roles, responsibilities, and lines of communications that report to a single management focal point.

Comment

We defer comment on a single management focal point until our new CIO has the opportunity to review the issue. We agree that we need to clearly delineate roles, responsibilities, and lines of communications. We will convene a workgroup to review any underlying issues and make recommendations as appropriate.

Recommendation 3

Ensure the CIO is delegated with sufficient authority and provided sufficient resources to fulfill his security responsibilities according to applicable laws, regulations, and guidance.

Comment

We defer comment on sufficient delegated authority and resources until our new CIO has the opportunity to review the issue. We do support providing additional resources to the CIO for use in fulfilling his security responsibilities.

Recommendation 4

Update the agency-wide Information Security Program Plan.

Comment

We agree. The CIO's office is currently reviewing and updating both our agency-wide Information Security Program Plan and our IT Security Strategic Plan. We will be sure to align both documents. We have already aligned our IT Security Strategic Plan with our agency Strategic Plan.

Recommendation 5

As appropriate, ensure written policies and procedures require notification of all agency systems users of certain computer incidents.

Comment

We agree. Agency policy requires that we maintain computer incident response capability. We are updating the Incident Reporting Handbook to reflect the responsibilities of our security response team in notifying all agency systems users, as appropriate, of computer incidents.

We also include computer incident notification procedures in the Office of Systems/Office of Telecommunications and Systems Operations incident response documentation. These procedures should be included in the Information Systems Security Handbook only as a reference to the Office of Systems managed documentation. Exposing the procedures to more individuals increases the risk for misuse and it may desensitize employees to the message delivery vehicle if used too frequently.

Recommendation 6

Update the Information Systems Security Handbook (ISSH) with the most current and accurate information and consider further delineating security roles and responsibilities of our agency components and security officers related to the subject matter in each chapter. We should include all security policies or references in the ISSH.

Comment

We agree. We are updating and restructuring the ISSH to include all security policies, references, accurate organizational names, and reporting relationships. We will further delineate the security roles and responsibilities as appropriate.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Acting Director, Information Technology Audit Division

Phil Rogofsky, Audit Manager

Mary Ellen Moyer, Audit Manager

Acknowledgments

In addition to those named above:

Grace Chi, Auditor-in-Charge

Tina Nevels, 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-14-09-19048.

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, 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.