OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S MANAGING AND MONITORING OF LOCAL PROFILES

July 2011 **A-14-10-20106**

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: July 13, 2011 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Managing and Monitoring of Local Profiles (A-14-10-20106)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) managing and monitoring of nonfinancially significant local profiles[1] compromised the security of its information; information systems; personnel; or other resources, operations, or assets.

BACKGROUND

SSA policy states that controlling and limiting access to the Agency's information systems and resources is the first line of defense in ensuring the confidentiality, integrity, and availability of the Agency's information technology (IT) resources.[2]

SSA's systems access policy is built on the access control principles of least privilege[3] and need to know.[4] SSA uses TOP SECRET, a commercial access control package modified to fit SSA's unique requirements, to control access to SSA's computer

[1] We define nonfinancially significant local profiles as profiles that allow access to datasets in applications that would not materially affect SSA's financial statements. Profiles that allow update or greater access to datasets in applications that would materially affect SSA's financial statements are defined as financially significant.

[2] SSA, *Information Systems Security Handbook (ISSH)*, version 1.5, section 2.1, Systems Access Policy: Purpose, page 9.

[3] Granting users access only to the applications, transaction screens, and information systems they need to perform their official duties.

[4] The legitimate requirement of a person or organization to know, access, or possess sensitive or classified information that is critical to the performance of an authorized, assigned mission.

systems. The Agency's users must have an identification (ID), password, and profile[5] to gain access to SSA's computer systems.

IDs and Passwords

SSA has two types of IDs: a personal identification number (PIN) for those who need to access SSA's computer systems and a User Identification (UserID) that is primarily for technical personnel. Additionally, a subset of technical personnel who may need to update files or records in a production dataset[6] do so by using an additional, restricted UserID, called a secondary UserID. The secondary UserID allows the Agency to monitor those with update access to its production datasets.

Profiles

Profiles provide the Agency an effective way of grouping users who share common system access needs, while maintaining individual accountability necessary for a secure computer environment. The Agency groups users by basic job positions and creates positional profiles[7] for each of these basic jobs. For example, a claims representative has a claims representative positional profile. To comply with the principles of least privilege and need to know, SSA's security officers[8] assign a positional profile to every user's PIN. Security officers assign a positional profile to those users who also have UserIDs.

Another type of profile is the functional profile, which the security officer can assign to PINs or UserIDs. Functional profiles allow users to perform specific duties by granting access to just those transactions or data files needed to accomplish a function not addressed by their positional profile. Some users may have multiple functional profiles assigned to their PIN/UserID in addition to their positional profile. For example, we found that staff who had functional profiles granting them greater than read access to datasets had more than one functional profile assigned to their UserID.

Profiles can also be categorized by ownership. Profiles are either corporate or local. A corporate profile has gone through multiple component processes and approvals to ensure proper access to IT resources. A security officer cannot directly create or modify a corporate profile. Instead, the security officer must submit any profile creation or modification request through the multi-component approval process. The Agency

---

[5] Standardized Security Profile Project (SSPP), Building Production Dataset Profiles, version 2.2, pages 2 and 3.

[6] A dataset is a collection of logically related data records and can contain application data or information such as source programs, macro libraries, and system variables. Applications that are critical to the Agency's daily business use production datasets.

[7] A positional profile determines what access to systems resources each position needs.

[8] The security officers are the individuals responsible for implementing SSA's security policies within their respective component.

considers any profile that goes through this formal, multi-component approval process to be locked-down.

Unlike corporate profiles, which are owned by the Office of Telecommunications and Systems Operations, each Agency component can create and own local profiles. SSA does not consider local profiles locked-down because the profile did not go through the formal, multi-component approval process. Some components have a business need to maintain a number of local profiles for technical personnel to make emergency changes to systems, applications, or data. At times, components use local profiles because the formal, multi-component approval process for a corporate profile cannot always be completed in time to meet the emergencies that occur.

PRIOR AUDIT FINDINGS

Our Fiscal Year (FY) 2009 financial statement audit identified a significant deficiency[9] in the Agency's control of access to its information. We reported that the IT resources contained in both corporate and local profiles were not reviewed periodically. In addition, testing disclosed the Agency could not ensure that employees and contractors were given least privilege access to perform their job responsibilities. Thus, we recommended that SSA implement a policy requiring a periodic review of profile contents. In the FY 2010 financial statement audit, Grant Thornton, LLP continued to identify a significant deficiency in SSA's access controls to its information.[10] The auditors continued to report the significant deficiency because the Agency had not completed its efforts to correct the access control weaknesses identified in FY 2009.

One of the weaknesses reported in FY 2009 stated that the Agency had not properly managed and monitored financially significant[11] local profiles. Our testing of FY 2009 nonfinancially significant local profiles was limited; therefore, we initiated this review to determine whether nonfinancially significant local profiles compromise the security of the Agency's information; information systems; personnel; or other resources, operations, or assets. Although we limited the focus of this review to SSA's management and monitoring of nonfinancially significant local profiles, our prior financial statement audit work identified similar access control weaknesses for financially significant profiles (both local and corporate).

To achieve our objective, we randomly selected and examined a number of nonfinancially significant local profiles. For more information about our scope and methodology and our sampling methodology, see Appendices B and C, respectively.

---

[9] SSA OIG, *Fiscal Year 2009 Financial Statement Audit* (A-15-09-19124), November 9, 2009.

[10] SSA OIG, *Fiscal Year 2010 Financial Statement Audit Oversight* (A-15-10-10113), November 8, 2010.

[11] See Footnote 1.

RESULTS OF REVIEW

In our review of SSA's process for managing and monitoring nonfinancially significant local profiles, nothing came to our attention that compromised the security of the Agency's information; information systems; personnel; or other resources, operations, or assets. Although the population of local profiles decreased from 2009 to 2010 and the Agency plans to decrease them further, any mismanagement of these profiles could present an opportunity for those knowledgeable of access control vulnerabilities to compromise SSA data. We believe the possibility of a compromise will diminish if SSA implements its plans to decrease the number, and restrict the use of, local profiles.

Further, SSA has made significant improvements regarding its management and monitoring of local profiles; however, more improvements are needed. We found SSA could improve its profile certification process by obtaining nonuse information about profiles. Additionally, SSA needs to develop a secondary UserID control policy that is clear, concise, and consistent.

AGENCY PROGRESS TO IMPROVE ITS MANAGEMENT AND MONITORING OF PROFILES

SSA made significant improvements regarding its management and monitoring of local profiles. During its work on the FY 2009 Financial Statement Audit,[12] PricewaterhouseCoopers, LLP found that SSA had approximately 3,500 local profiles and 4,600 corporate profiles. In SSA's FY 2009 *Performance and Accountability Report*, the Agency described a significant deficiency identified by the OIG that related to weaknesses in controls over information security.[13]

In August 2010, the Agency's local profile inventory had decreased to approximately 1,400, and corporate profiles increased to about 5,700. SSA decreased the local profiles by converting them to corporate status or deleting local profiles no longer needed. Part of the increase in the number of corporate profiles was due to the Agency's efforts to lock down its local profiles and change the ownership status from local to corporate. From August 27, 2009 to August 23, 2010, SSA reduced the number of local profiles by about 60 percent.

Additionally, the Office of the Chief Information Officer plans to announce in Calendar Year 2011 a new policy that will decrease the number and restrict the use of local profiles. We believe such a strategy would greatly mitigate the concerns identified in this report. In addition, the Office of the Chief Information Officer is leading an Agency workgroup to recommend revised policy and entity-wide procedures to govern the administration and review of all production security profiles by September 2011. We recommend that the Agency continue with its plans to reduce the number and restrict the use of local profiles.

---

[12] *SSA's FY 2009 Performance and Accountability Report*, November 2009.

[13] Id. at 43.

While we commend the Agency for taking these actions, improvements are still needed. The following findings contain recommendations needed to improve SSA's management of local profiles. Furthermore, to the extent that any of the conditions identified in the following findings are applicable to the management of corporate profiles, SSA should consider similar corrective action. We found the Agency could improve its profile certification process by obtaining nonuse information about local profiles. Additionally, SSA needs to ensure consistency in its policies related to assigning local profiles to secondary UserIDs.

NONUSE OF LOCAL PROFILES, DATASETS, AND USERIDS

Adhering to the principles of least privilege and need to know helps reduce the risk of compromising the confidentiality, integrity, or availability of SSA's IT resources. One of the ways SSA enforces compliance with these access control principles is through its Triennial Certification (TEC) process.

During the TEC process, managers review the profiles (including both corporate and local) assigned to each of their employees and determine whether the employees have only those profiles needed to do their jobs. If the managers determine their employees no longer need a profile, they are supposed to instruct the security officer to remove the profiles from the employees' PINs and UserIDs. SSA performed its most recent large-scoped TEC from June 1 to July 30, 2009. After our fieldwork, the Agency informed us that it did a smaller-scoped TEC in 2011. We did not confirm the results of the TEC.

To examine the status of nonuse of local profiles, we obtained an IT Resource Usage Report[14] as of September 2, 2010 from SSA's Office of Telecommunications and Systems Operations for 41 local profiles in our sample of 100. Collectively, these 41 profiles granted 385 users access to 944 datasets through UserID accounts. Some of these 385 users had access to more than 1 of the 41 profiles. We used the data obtained to determine the nonuse status as of the date the TEC began.

Although SSA conducted its last large-scoped TEC in 2009, we found that some SSA employees had not accessed their local profiles for at least 1 year before the TEC and still had not accessed their local profile over 1 year later when we performed our test. Many datasets linked to the employee's profile had not been accessed for at least 1 year before the TEC, and these employees still had not accessed the datasets for over 1 year after the TEC. In addition, we found several resources that users never accessed.

[14] The eTrust Cleanup report (IT Resource Usage Report) shows a profile's and UserID's last date of access. For any profile or UserID input, the report lists how many days have elapsed since the date of last usage (Date Referenced column). We used the term "never used" if the profile or UserID did not have an entry in the Date Referenced column. In these instances, the report showed how many days have elapsed (Days Unused column) since that resource was registered (Date Loaded column). It is possible that those profiles we described as "never used" were used before the date in the Date Loaded column.

IT Resources with Nonuse Exceeding 1 Year Existed When the 2009 TEC Began

We found periods of nonuse greater than 1 year for a subset of the 41 profiles that collectively granted access to 944 datasets to 385 users. Table 1 summarizes nonuse of these profiles, datasets, and users as of the 2009 TEC.

Table 1- Summary of Nonuse by Elapsed Timeframes

	Description\Resource Category	Profiles	Datasets	Users
1	Not used for at least 3 to 4 years[15] as of June 1, 2009 (Includes 4 profiles never accessed)	4	282	44
2	Not used for at least 2 to 3 years as of June 1, 2009 (Includes 1 profile never accessed)	2	43	26
3	Not used for at least 1 to 2 years as of June 1, 2009 (Includes 1 profile never accessed)	3	53	21
4	Total Nonuse for at least 1 year	9	378	91

The Nonuse of IT Resources Continued to Increase After the 2009 TEC. Table 2 compares the nonuse information as of the 2009 TEC and the September 2010 IT Resource Usage Report. It shows that 15 months after June 1, 2009, the number of resources that had elapsed times of at least 1 year had increased. Every profile, dataset and user count shown in row 1 of Table 2 is included in the counts in row 2. In every case, if nonuse exceeded 1 year as of the 2009 TEC date, the nonuse continued for another 15 months.

Table 2- Comparison of Nonuse Elapsed Time

	Description\Resource Category	Profiles	Datasets	Users
1	Number per Resource Category not used for at least 1 year as of June 1, 2009 (TEC)	9 of 41 (22 percent)	378 of 944 (40 percent)	91 of 385 (24 percent)
2	Number per Resource Category not used for at least 1 year as of as of September 2, 2010 (IT Resource Usage Report)	14 of 41 (34 percent)	600 of 944 (64 percent)	153 of 385 (40 percent)

Some IT Resources Had Never Been Accessed. Table 3 compares IT resources never accessed as of the 2009 TEC and the September 2010 IT Resource Usage Report. The Table shows an increase in the number of resources never accessed during the 15 months after June 1, 2009.

[15] The registration date for the four profiles never accessed was June 7, 2005, or almost 4 years before the 2009 TEC start date. The creation dates for these four profiles are earlier than June 7, 2005, so the nonuse period for these four profiles could be even longer than 4 years.

Table 3- Comparison of Never Used Time Greater Than 1 Year

	Description\Resource Category	Profiles	Datasets	Users
1	Number per Resource Category never used for at least 1 year as of June 1, 2009 (TEC)	6 of 41 (15 percent)	294 of 944 (31 percent)	64 of 385 (17 percent)
2	Number per Resource Category never used for at least 1 year as of as of September 2, 2010 (IT Resource Usage Report)	7 of 41 (17 percent)	443 of 944 (47 percent)	101 of 385 (26 percent)

During the TEC, we believe employees who have not used their profiles or accessed datasets within their profiles for at least 1 year should have their access needs reviewed. Although we state a nonuse period of at least 1 year as a basis for initiating a review, the Agency should determine what constitutes a nonuse period as a basis for review. Allowing employees access to data not needed for their job responsibilities increases the risk of compromising the confidentiality, integrity, and availability of SSA's data.

We recommend SSA periodically review the IT Resource Usage Report to identify individuals whose periods of non-access warrant further review for continued access. Based on management's review of the IT Resource Usage Report, management could authorize SO to modify or revoke access, if needed, to comply with the access control principles of least privilege and need to know.

INCONSISTENCIES IN SECONDARY USERID CONTROL POLICIES AND PROCEDURES

Our sample of 100 local profiles included 41 that granted access to datasets for 384 users.[16] We reviewed 34 of these 41 profiles and found 29 that granted 172 users update or greater access to datasets through primary UserIDs.[17] The Agency's ISSH[18] states, "Update or greater access is accomplished via a user approved secondary UserID which is activated only for the period needed, and this activity is audited."

The policies in the ISSH[19] pertain to all SSA employees and contractors. The ISSH does not distinguish between local or corporate profiles. We identified 29 profiles where SSA did not comply with its ISSH policy[20] because users' profiles were not assigned to a secondary UserID. By not assigning a secondary UserID, the Agency had limited

[16] The difference of 1 between the 384 users and the 385 users on pages 5 through 7 and Appendix C was due to a timing difference. The profiles had 384 users for the data received in May 2010 and 385 users for the data received in September 2010.

[17] Of the five remaining profiles, one had been deleted and nonuse data was not available for six users. We found 1 profile where 2 users properly used the secondary UserID and the other 3 granted 32 users read-only access to datasets, so no secondary UserIDs were needed.

[18] SSA ISSH, supra, Section 2.3, Policy at page 9.

[19] SSA ISSH, supra, Section 1.1, Overview of IT Security at page 5.

[20] SSA ISSH, supra, Section 2.3, Policy at page 9.

ability to monitor the users' activities and therefore the users could make unwarranted or erroneous changes to SSA's data.

These 29 profiles were issued by 6 components. We asked representatives from each component why they did not use the secondary UserID process. For 28 of the 29 profiles, the representatives stated that the secondary UserID control process did not apply or its use would hinder productivity. The representative for the remaining profile stated that the profile no longer granted update or greater access.

Our review of SSA's secondary UserID policies and procedures identified conflicting scopes and undefined terminology that may have contributed to inconsistent compliance with secondary UserID policy. For example, SSA's ISSH, Chapter 2, provides limited high-level secondary UserID policy.[21] ISSH, Appendix I,[22] provides additional guidance; however, it contradicts Chapter 2. Chapter 2 requires that individuals granted update or greater access use a secondary UserID.[23] Appendix I restricts the use of the secondary UserID to programmers granted update access to production datasets via Standardized Production Profiles.[24] In addition, neither Chapter 2 nor Appendix I defines production datasets or Standardized Production Profiles. Appendix I does provide a link to the SSPP Intranet home page for readers to find the secondary UserID procedures.

We found five pages on SSA's Intranet that provided additional secondary UserID policies and procedures. We determined the policies and procedures used different and undefined terms to describe the scope and application of the secondary UserID process; used different names for the secondary UserID; and disagreed on the type of access (full versus emergency) and duration of the emergency access required for assigning secondary UserIDs.

Based on our findings, we believe the Agency should resolve the inconsistencies among its policies and procedures and better describe and define the secondary UserID control policy, standards, and procedures. We recommend SSA develop a secondary UserID control policy that is clear, concise, and consistent.

---

[21] SSA ISSH, supra, section 2.3, at page 9.

[22] SSA ISSH, Appendix I, *Systems Access Security Administration Software,* pages I-3 through I-4.

[23] SSA ISSH, supra, section 2.3, at page 9.

[24] SSA ISSH, supra, Appendix I, *Systems Access Security Administration Software,* section E at page I-3.

CONCLUSION AND RECOMMENDATIONS

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

In our review of SSA's process for managing and monitoring nonfinancially significant local profiles, nothing came to our attention that compromised the security of the Agency's information; information systems; personnel; or other resources, operations, or assets. Although the population of local profiles decreased from 2009 to 2010 and the Agency plans to decrease them further, any mismanagement of these profiles could present an opportunity for those knowledgeable of access control vulnerabilities to compromise SSA data. We believe the possibility of a compromise will diminish if SSA implements its plans to decrease the number, and restrict the use, of local profiles. In addition, we did identify some areas that needed improvement.

As such, we recommend that the Agency:

1. Continue with its plans to reduce the number, and restrict the use, of local profiles.

We recommend the following strategies to improve SSA's managing and monitoring of local profiles. Furthermore, to the extent that any of the conditions identified in this report are applicable to the managing and monitoring of corporate profiles, SSA should consider similar corrective action. As such, we recommend SSA:

2. Periodically review the IT Resource Usage Report to identify individuals whose periods of non-access would warrant further review for continued access. Once reviewed, modify or revoke access, if needed, to comply with the access control principles of least privilege and need to know.

3. Develop a secondary UserID control policy that is clear, concise, and consistent.

AGENCY COMMENTS

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

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

FY	Fiscal Year
ID	Identification
ISSH	*Information Systems Security Handbook*
IT	Information Technology
OIG	Office of the Inspector General
PIN	Personal Identification Number
SSA	Social Security Administration
SSPP	Standardized Security Profile Project
TEC	Triennial Certification
UserID	User Identification

Scope and Methodology

To accomplish our objective, we:

- Obtained and reviewed pertinent Federal criteria governing access controls.
- Obtained and reviewed pertinent Agency policy and procedures governing the authorization, creation, modification, and usage of local profiles.
- Interviewed key staff from components reporting to the Deputy Commissioner for Systems.
- Met with management in the Office of the Chief Information Officer to discuss profile security policies and procedures.
- Obtained extracts from the Agency's Office of Telecommunications and Systems Operations that contained 2,561 local profiles on the Profile Registry reports as of March 16 and August 23, 2010.
- Compared the March 16, 2010 extract to the extract obtained by PricewaterhouseCoopers, LLP on August 27, 2009.
- Selected a random sample of 100 local profiles from the March 16, 2010 Profile Registry report (see Appendix C).

We conducted our audit between January and November 2010 in Baltimore, Maryland. We found the data used for this audit to be sufficiently reliable to meet our audit objective. The primary entity audited was the Office of Systems.

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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sampling Methodology

To accomplish our sampling objective, we:

- Obtained a data extract from the Agency of 2,561 local profiles as of March 16, 2010.

- Excluded from possible testing 1,028 local profiles in existence as of March 16, 2010 that
  - PricewaterhouseCoopers, LLP tested in Fiscal Year 2009;
  - appeared to access non-production datasets (names contained such terms as integration, test, or training);
  - did not access any datasets; and,
  - security officers had not assigned to any users.

- Selected a random sample of 100 local profiles from the audit population of 1,533.

- Tested one local profile that granted user identification (UserID) access to datasets from the Human Resources Management Information System.

- Obtained a TOP SECRET WHOHAS report for each profile in our sample as of May 24, 2010. This report contains various information about each profile, such as profile creation date, profile ownership, datasets assigned, the dataset access level allowed, and UserIDs granted access.

Based on our analysis of the TOP SECRET data, we determined that 41 of the 100 profiles in existence as of March 16, 2010 had been accessible to 384 users as of May 24, 2010.

Because of time constraints, we could not test all 100 profiles in the sample. Instead, we tested the 41 profiles that were still granting access to datasets as of May 24, 2010. The remaining 59 profiles had been modified since our March 16, 2010 data extraction and no longer granted users access to datasets.

From August through September 2010, we queried the TOP SECRET Administrator's security administration database to determine which of these 41 profiles were still in local profile status and how many users had secondary UserIDs.

On September 2, 2010, we obtained a listing from the TOP SECRET eTrust Cleanup utility for the 41 profiles, 944 datasets and the 385 users to determine the number of elapsed days since a profile was last accessed, a dataset was last accessed via that profile, and a user last accessed that profile.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: June 24, 2011 Refer To: S1J-3

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

From: Dean S. Landis /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, "The Social Security Administration's Managing and Monitoring of Local Profiles" (A-14-10-20106)--INFORMATION

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

Please let me know if we can be of further assistance. You may direct staff inquiries to Frances Cord at (410) 966-5787.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S MANAGING AND MONITORING OF LOCAL PROFILES" (A-14-10-20106)

Recommendation 1

Continue with its plans to reduce the number, and restrict the use, of local profiles.

Response

We agree.

Recommendation 2

Periodically review the IT Resource Usage Report to identify individuals whose periods of non-access would warrant further review for continued access. Once reviewed, modify or revoke access, if needed, to comply with the access control principles of least privilege and need to know.

Response

We agree.

Recommendation 3

Develop a secondary UserID control policy that is clear, concise, and consistent.

Response

We agree.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Grace Chi, Acting Audit Manager

Acknowledgments

In addition to those named above:

Alan Lang, Senior Auditor

For additional copies of this report, please visit our Website at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Staff Assistant at (410) 965-4518. Refer to Common Identification Number A-14-10-20106.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

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

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

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

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

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

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

Chairman and Ranking Minority Member, Committee on Finance

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

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

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

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

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

Office of Technology and Resource Management

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