OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

ASSESSING THE APPLICATION CONTROLS FOR THE SOCIAL SECURITY ADMINISTRATION'S INTEGRATED DISABILITY MANAGEMENT SYSTEM

March 2006 **A-14-05-15064**

AUDIT REPORT

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the 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

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

MEMORANDUM

Date: March 23, 2006 Refer To:

To: The Commissioner

From: Inspector General

Subject: Assessing the Application Controls for the Social Security Administration's Integrated Disability Management System (A-14-05-15064)

OBJECTIVE

Our objective was to assess the application controls for the Social Security Administration's (SSA) Integrated Disability Management System (IDMS). The audit encompassed the three phases of the processing cycle (input, processing, and output) to ensure disability-related transactions are valid, properly authorized, and completely and accurately processed and reported.

BACKGROUND

SSA established the IDMS in 2002 as a central repository for disability information for all Title II and Title XVI beneficiaries. Its purpose is to enhance management of post-entitlement disability processing. This would include the medical continuing disability review (CDR) process and meeting the requirements set forth in the Ticket to Work legislation.[1] The IDMS provides online access to all disability-related information for a beneficiary's or recipient's work and earnings, Ticket to Work status, and data regarding pending and processed CDRs and expedited reinstatement actions. IDMS provides on-line access and integrates the following disability-related databases and systems: Disability Control File, Ticket Payment File, Earnings File, and the Employment Network payment system. SSA controls on-line access to IDMS through the use of specialized software.

[1] Ticket to Work and Work Incentives Improvement Act of 1999, Pub. L. No. 106-170, 113 Stat. 1860. (1999).

Access Control Software

SSA uses eTrust® CA-Top Secret (Top Secret), a commercial access control software package, to control employee access to IDMS and other production[2] mainframe computer resources. Top Secret protects computer resources by identifying authorized users and controlling their access capability via individual personal identification numbers (PIN). The PIN is assigned as many profiles as the employee needs to perform his or her job duties.

One of Top Secret's primary mechanisms for controlling user access is the access authorization profile. Profiles contain sets of common access authorizations referred to as transaction identifications (ID) for groups of users. Access authorizations allow specific data entry transactions and query capabilities for each computer screen.

Another mechanism for controlling access is via datasets. Datasets are groups of related electronic files containing data and/or programs. Dataset access can be granted to PINs or to profiles that permit the user to read, update, change, or delete the data or programs stored in the files.

We identified 289 access authorization profiles assigned to 69,548 individuals with PINs providing access to the IDMS application. Access authorization profiles are profiles that are reviewed, approved, and administered by SSA's Office of Systems Security Operations Management (OSSOM). These profiles are most applicable to operational positions, such as benefit authorizers, that are standard throughout SSA's field locations.

Concept of "Least Privilege"

SSA has incorporated the principle of "least privilege" as a standard in its Information Systems Security Handbook (ISSH). In fact, the ISSH[3] states that controlling and limiting access "…is the first line of defense in assuring the security, integrity and availability of the Agency's information systems and resources." Least privilege is defined as the practice of restricting a user's access to data files, processing capabilities, or type of access (such as, read, write, execute, delete) to the minimum necessary to perform his or her job.

Since the 1997 audit of SSA financial statements, the related internal control report contained a reportable condition related to information protection, which included the Agency's ability to effectively implement the concept of least privilege. During the 2005 audit, SSA's financial statement audit contractor removed a reportable condition

[2] Production mainframe computer resources consist of files and datasets, software applications, and programs that operate in SSA's primary business operating environment.

[3] ISSH, Chapter 10, *Systems Access Security*, page 1 (September 2004).

regarding security access authorizations. This decision was based on improved access controls for eleven applications critical to the financial statements. To resolve the reportable condition, SSA implemented (1) the Standardized Security Profile Project to address programmer access issues, and (2) periodic reviews of Office of Operations access authorizations based on least privilege. IDMS was not one of these critical systems. However, SSA plans to expand its efforts to include non-critical systems in the future. This report includes a review of not only programmer access, but also a full review of access authorizations for all Agency components, including the Office of Operations.

RESULTS OF REVIEW

We reviewed the significant input, processing, and output controls for the IDMS. While we found many processing and output controls were strong and operating effectively, we identified areas where input controls should be improved. We tested two areas of input controls: input edits and system access. Our review determined that input edits were effective, but system access needs to be strengthened.

Access Controls Need to be Strengthened

We found the following issues with access controls:

- Excessive Access was Granted to IDMS Data via Transaction IDs.
- Excessive Access to Production Datasets.
- Process for Bypassing Edits Lacks Adequate Controls.

Excessive Access was Granted to IDMS Data via Transaction IDs

Excessive access to IDMS data was granted via Top Secret transaction IDs. Specifically, transaction IDs were assigned to Top Secret profiles that were not necessary for employees to perform their job responsibilities; thereby, resulting in excessive access. We found 84 of 289 IDMS Top Secret access authorization profiles were assigned to 23,136 individuals who were granted excessive access to the IDMS application and data. SSA's policy of "least privilege" requires access be limited to the "minimum necessary" to perform one's job responsibilities.

These access permissions allow (1) CDR establishment, (2) changes to medical data and diary dates, and (3) changes to bank account and routing numbers for payments to Employment Network vendors. Additionally, this level of access could result in erroneous decisions regarding CDRs and Ticket to Work issues because of inappropriate changes to the data.

According to the ISSH,[4] it is the responsibility of management to determine and approve the access needs of their employees. Changes to employees' access are requested by management via a profile access matrix, approved by the component security officer (CSO) and delivered to the OSSOM staff for final authorization.

Security officers are responsible for the development, implementation, and management of a security program within their organization.[5] Security officers also administer the assignment of PINs, passwords and profiles to ensure employees have access to only those system resources necessary to perform their assigned responsibilities.[6] Some security officers need further guidance to (1) select and properly assign appropriate transaction IDs to profiles, (2) adequately understand the capabilities of the transaction IDs involved, and (3) adequately understand the job requirements in their respective components for requesting appropriate access. For example, in the Office of Hearings and Appeals (OHA) and the Office of the Chief Actuary, security personnel inadvertently or unknowingly assigned transaction IDs that provided the capability to update or modify data in IDMS, when query-only access was all that was needed.

The 84 profiles with excessive access belonged to 10 SSA components. After discussions with each of the CSOs, all agreed that access was excessive and eight (OHA, Office of Disability Operations, Office of Disability and Income Security Programs, Office of Disability and Supplemental Security Income Systems, Office of International Operations, Office of Public Service and Operations Support, Office of Quality Assurance, and Office of Telecommunications and Systems Operations) initiated appropriate profile changes during our audit. We believe excessive access was granted because of the following reasons.

1. **CSOs were not familiar enough with the IDMS application to properly assign update or query-only access.** Several security officers stated that when they assigned access to the application, they allowed users to decide access levels, or they simply copied profiles from other components. Other CSOs stated they or their security staff simply did not have the in-depth knowledge of the application area to be able to assign the appropriate access levels.

2. **Inadequate review of Top Secret profiles.** OSSOM staff reviews and approves all new or modified access authorization profiles before they are implemented. During its profile reviews, OSSOM staff did not detect or prevent the erroneous IDMS transaction IDs from being assigned.

[4] ISSH, Chapter 10, *Systems Access Security*, page 12 (September 2004).

[5] ISSH, Chapter 2, *Security Officer Standards*, page 1 (February 2001).

[6] ISSH, Chapter 2, *Security Officer Standards*, page 4 (February 2001).

3. **Security officers did not always attend the Security Kickoff meetings.** Two CSOs did not attend these security meetings or send an alternate. Security Kickoff meetings are held by CASB in conjunction with systems development staff to provide detailed security information and answer questions regarding security access to each application when either a new application is being released or when there are significant changes to an application. If the component will require access to the application, CSOs should be strongly encouraged to either attend all Security Kickoff meetings, or send an alternate.

4. **Thirty-eight of 57 IDMS transaction IDs in the Top Secret Resource List were not clearly identified as having "update" or "query-only" capability.** SSA should ensure clear labeling of transaction IDs identifying the type of access they bear to help ensure excessive access is not erroneously granted.

Excessive Access to Production Datasets

We identified 14 programmers and analysts in the Office of Systems (OS) who had the "All" access designation within the Top Secret security software to IDMS datasets. The "All" access designation allows users to create, delete and modify any of the data contained within the datasets we reviewed. This level of access prevents SSA from ensuring the integrity of IDMS because data could be inadvertently or intentionally updated, changed, or deleted by unauthorized individuals. By allowing programmers and analysts to have the "All" access designation, SSA is not conforming to Office of Management and Budget (OMB) Circular No. A-130 Appendix III, *Security of Federal Automated Information Resources,*[7] concept of least privilege or separation of duties. As noted earlier, SSA has taken steps to remove programmer access to production datasets for its critical systems, and plans to expand this process to other systems, including IDMS, in the future.

SSA was unaware that these 14 programmers and analysts had update access. SSA was unable to determine why this access occurred because this access had been in existence for an indeterminate period of time. SSA should modify dataset access to be "read only" and instruct staff to use SSA's procedures for accessing production datasets via the "Second $UserID"[8] process.

During the course of our audit, SSA began to modify the IDMS production dataset access of these programmers and analysts to "read only" and implement the "Second $UserID" process per our recommendation. SSA has not yet completed this process.

[7] OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, section B(a)(2)(c).

[8] The Second $User ID procedure was developed to comply with the requirements of OMB Circular No. A-130 by allowing application programmers temporary update access privileges to address system anomalies.

Process for Bypassing Edits Lacks Adequate Controls

SSA's Office of Employment Support Programs (OESP) processes payments to the Employment Network vendors under the Ticket to Work program via the IDMS. The IDMS permits authorized users to process payments that meet certain requirements as determined by Agency policy. However, if one of the requirements is not met, IDMS will display a ticket payment edit when the user attempts to input the data to the system. The presence of an edit message also prevents further processing until the condition that created the edit message is rectified. For example, IDMS normally will display an edit message and prevent further payment processing when an employer was already paid for the timeframe requested or when benefit payments have been suspended to the beneficiary or recipient for medical reasons.

As part of its July 2005 software release, by request of the business owner, OS programmed the capability for some Ticket payment edits to be bypassed. Consequently, IDMS will now permit users whose PINs are listed in a particular dataset to bypass three Ticket payment edits and allow further processing of payment requests to Employment Network vendors under the following conditions:

- A Ticket payment request for a terminated Ticket.
- A Ticket payment for a milestone claim for a beneficiary who is not in current payment status.
- A Ticket payment for an outcome claim for a beneficiary who is still receiving benefits.

OESP staff sometimes has a legitimate business need to bypass these edits, such as when data on the IDMS database is incorrect. As of September 8, 2005, six individuals in OESP had the ability to bypass these three edits, and only five were in need of this ability.[9] However, the dataset that controls who has the ability to bypass these edits can be updated, changed, or modified at any time by seven individuals in OS. Changes, updates, and modifications to this file are not captured, monitored, or tracked through an audit trail. As a result, inappropriate individuals could be added to the file and have the ability to bypass these edits. This level of access prevents SSA from ensuring that erroneous, inaccurate or improper payments to Employment Network vendors are not made. This occurred because SSA did not design the application with the capability to make corrections or perform overrides.

While we understand the need for certain edits to be bypassed to process transactions correctly, we believe SSA can mitigate the risks by implementing compensating controls. To improve controls, SSA should remove "All" access to this dataset and instruct staff to use SSA's procedures for accessing production datasets via the

[9] We discovered that the sixth individual no longer worked for the component and consequently, no longer needed access. SSA removed his access on September 14, 2005.

“Second $UserID” process. If cost effective, SSA should modify the IDMS software to achieve this functionality rather than modifying input controls using dataset access.

During the course of our audit, SSA has begun to modify the dataset access of these programmers and analysts to “read only” and implement the “Second $UserID” process per our recommendation. SSA has not yet completed this process.

CONCLUSION AND RECOMMENDATIONS

SSA needs to strengthen security access controls for the profiles that have excessive access. Excessive access could result in erroneous decisions regarding CDRs and Ticket to Work issues; erroneous, inaccurate or improper payments to Employment Network vendors; and the loss of data. To establish proper security controls and effectively implement the policy of least privilege, SSA needs to restrict authorized employee access to that which is needed to perform assigned duties. SSA also needs to improve security officers’ monitoring and oversight in the granting of access throughout SSA.

We recommend SSA:

1. Remove excessive or inappropriate transaction IDs from those profiles identified as having excessive access.

2. Enforce the policy of least privilege by following existing policy and conducting more thorough reviews of security access matrices.

3. Strongly encourage CSOs (or their alternates) to attend those IDMS Security Kickoff meetings when access will be requested.

4. Ensure the labeling of IDMS transaction IDs in the Top Secret Resource List clearly identifies the type of access they bear, whether “update” or “query-only.”

5. Continue to ensure that programmer access to production datasets is controlled via the “Second $UserID” process.

6. If cost effective, SSA should modify the IDMS software to allow for ticket corrections, so that edits no longer need to be bypassed.

AGENCY COMMENTS

SSA agreed with our recommendations. See Appendix D for the full text of the Agency's comments.

Patrick P. O'Carroll, Jr.

Appendices

Appendix A

Acronyms

CASB	Control Audit, and Security Branch
CDR	Continuing Disability Review
CSO	Component Security Officer
ID	Identification
IDMS	Integrated Disability Management System
ISSH	Information Systems Security Handbook
OESP	Office of Employment Support Programs
OHA	Office of Hearings and Appeals
OMB	Office of Management and Budget
OS	Office of Systems
OSSOM	Office of Systems Security Operations Management
PIN	Personal identification number
SSA	Social Security Administration

Background

The online portion of the Integrated Disability Management System (IDMS) consists of 57 unique online screens on which users can establish a continuing disability review (CDR), input CDR decisions, update medical and diary information, add or delete Ticket assignments, initiate Ticket payments to Employment Network vendors, and change Employment Network information, including bank routing numbers for vendors. The IDMS contains data about disabled Title II beneficiaries and Title XVI recipients. IDMS serves as a data repository for all disabled individuals receiving benefits or working under the Ticket to Work incentives.

The IDMS is used in over 1,300 field offices nationwide, as well as Program Service Centers, Regional Offices, Teleservice Centers, Offices of Hearings and Appeals, and various Headquarters components, such as the Office of Disability and Income Security Programs, Office of Quality Assurance, and Office of the Chief Actuary. Thousands of SSA employees have some level of access to the IDMS—ranging from the ability to query very limited IDMS information to the capability for establishing and updating a full range of disability and employment data.

Concept of "Least Privilege"

The Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources*, requires that agencies: (1) maintain and protect individuals' identifiable information and proprietary information in a manner that precludes unwarranted intrusion upon personal privacy and violation of confidentiality; (2) ensure agency personnel are trained to safeguard information resources; (3) establish a level of security for all agency information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information system; and (4) ensure that only authorized personnel have access to information systems.

OMB Circular No. A-130 also requires that agencies incorporate personnel controls, such as separation of duties, least privilege, and individual accountability to ensure that adequate security is provided for an agency's major applications. Least privilege is defined as the practice of restricting a user's access to data files, processing capabilities, or type of access (such as, read, write, execute, delete) to the minimum necessary to perform his or her job. SSA has incorporated this principle as a standard in its Information Systems Security Handbook (ISSH).

SSA's Office of Systems Security Operations Management (OSSOM) staff, along with a network of regional and Central Office component security officers (CSOs), have overall responsibility to interpret, develop, and implement security policy. CSOs develop, implement, and manage the overall security program within their organizations, specifically administration of access controls. According to the ISSH,[1] OSSOM staff provides guidance and advises security officers in matters involving SSA's security program, establishes systems security policies and procedures, and administers the profile access authorization matrices.

SSA management has the overall responsibility to determine and approve the access needs of SSA employees. As part of this responsibility, management requests changes to employee access via the profile access authorization matrix to accommodate new developments or changes in circumstances. Changes to the profile access authorization matrices are reviewed and approved by the CSO and delivered to the OSSOM staff for final authorization. The types of profile changes that CSOs may request are:

- establishing a new profile for an employee position;
- adding a newly developed transaction identification (ID) to the profile access matrix;
- modifying an existing profile to add or remove a transaction ID; and
- deleting an existing profile.

SSA's Office of Systems' Control Audit, and Security Branch (CASB) makes recommendations on security, audit, and internal control issues for all SSA programmatic systems, including IDMS, ensures security standards are implemented, and leads reviews of programmatic processes and systems to identify security weaknesses. CASB validates and verifies matrices to ensure the requested access matches the access that is granted.

[1] ISSH, Chapter 10, *Systems Access Security*, page 2 (September 2004).

Scope and Methodology

To accomplish our objectives, we:

- Reviewed the applicable laws and Social Security Administration (SSA) regulations, rules, policies, and procedures.

- Reviewed 289 Top Secret access authorization profiles for the granting of access to the Integrated Disability Management System (IDMS). This included reviews of the Ticket to Work and Continuing Disability Review application profiles.

- Reviewed access to IDMS datasets and identified all PINs and profiles having excessive access.

- Reviewed the names for 57 transactions IDs listed in the Top Secret Resource List for the CDR and Ticket to Work applications.

- Interviewed SSA personnel in Headquarters components, including:

  - Office of the Chief Actuary,
  - Office of Disability and Income Security Programs,
  - Office of Finance, Assessment and Management,
  - Office of Operations,
  - Office of Policy, and
  - Office of Systems.

- Interviewed field office and program service center employees in Towson and Woodlawn, Maryland to ascertain user satisfaction and identify ongoing problems with the IDMS.

- Reviewed SSA's process for resolving, tracking, and monitoring the IDMS alerts in field offices.

Online Testing Environment

We tested 179 IDMS controls through online testing techniques. These techniques consisted of entering test transactions into a computer environment especially designed for audit testing purposes. The test system, created by SSA in June 2005, was separate and distinct from SSA's production mainframe system and was located on an isolated mainframe within SSA that had partial copies of production software and data. We conducted our testing between June 21 and August 4, 2005.

We developed our online tests based on established controls that were intended to be programmed in the system according to the system's detailed functional requirements, as well as on programmed controls that should exist to ensure actual results are achieved in accordance with overall SSA policy.

We performed our audit at Headquarters in Woodlawn, Maryland, and field locations listed above between April and October 2005. We conducted our audit in accordance with generally accepted government auditing standards.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: March 9, 2006 Refer To: S1J-3

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

From: Larry W. Dye /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "Assessing the Application Controls for the Social Security Administration's Integrated Disability Management System" (A-14-05-15064) – INFORMATION

We appreciate OIG’s efforts in conducting this review. Our comments on the draft report content and recommendations are attached.

Let me know if we can be of further assistance. Staff inquiries may be directed to Candace Skurnik, Director, Audit Management and Liaison Staff on extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "ASSESSING THE CONTROLS FOR THE SOCIAL SECURITY ADMINISTRATION'S INTEGRATED DISABILITY MANAGEMENT SYSTEM (IDMS)" (A-14-05-15064) -- INFORMATION

Thank you for the opportunity to review and comment on the draft report. We appreciate the comprehensive analysis demonstrated in this audit and take no issue with the findings. SSA takes very seriously our security responsibilities. We appreciate that the report makes note that components initiated appropriate profile changes during the course of the audit. In an effort to ensure compliance with the principle of "Least Privilege," we have initiatives underway to restructure the components' security profiles.

Our specific responses to the report's recommendations are provided below.

Recommendation 1

Remove excessive or inappropriate transaction IDs from those profiles identified as having excessive access.

Response:

We agree. To that end, several initiatives have been completed or are underway. For example, a revised matrix was submitted by the Deputy Commissioner for Operations (DCO) to correct the DCO profiles identified during the course of the audit. The Office of Systems Security Operations Management (OSSOM) continues to work with the Deputy Commissioner for Disability and Income Security Program's (DCDISP) Security Officer to ensure that the Ticket to Work program is adequately secured, including restricting user access in conformance to the contract and the principles of "need to know" and "least privilege."

Recommendation 2

Enforce the policy of least privilege by following existing policy and conducting more thorough reviews of security access matrices.

Response:

We agree. As noted in the report, Agency policy restricts user access to SSA information systems based on the principles of “need to know” and “least privilege.” To ensure compliance with Agency policy, OSSOM under the direction from the Chief Information Officer instructed managers working in concert with their component security officer (CSO) to review employee access to SSA systems at least once every three years, as well as when there is a change in employee job function or a change to a given application. This review will take place this fiscal year as a part of the Federal Information Security Management Act of 2002 compliance.

Recommendation 3

Strongly encourage Component Security Officers (CSOs), or their alternates, to attend those IDMS Security Kickoff meetings when access will be requested.

Response:

We agree. Consistent with Agency policy, CSOs and their alternates are expected to be entrenched in the life cycle development of Agency projects and applications, including participating in security kickoff meetings as discussed in the "Information Security Handbook" and echoed in the "Project Resource Guide" and the revised "Component Security Officer" guide.

Recommendation 4

Ensure the labeling of IDMS transaction IDs in the Top Secret Resource List clearly identifies the type of access they bear, whether “update” or “query-only.”

Response:

We agree. The Top Secret Resource List will be updated through our efforts to implement recommendations 1 and 2.

Recommendation 5

Continue to ensure that programmer access to production datasets is controlled via the “Second $UserID” process.

Response:

We agree. The Office of Systems scrutinized the batch profiles with remaining programmer access to production datasets. The "ALL" access has been removed from Primary $UserIDs and has been added to Second $UserIDs for a limited number of programmers.

Recommendation 6

If cost effective, SSA should modify the IDMS software to allow for ticket corrections so that edits no longer need to be bypassed.

Response:

We agree. The Office of Systems has updated, at DCDISP's request, the enhanced payment file that over-rides certain Employment Network (EN) Payment edits to limit access to designated Office of Employment Support Programs (OESP) users. The OESP Ticket/Disability Control File Program Advisor verifies the appropriateness of access for those persons who continue to have that access. Ticket to Work payment functionality has been improved significantly over the last calendar year. However, some cases remain that must be handled manually by OESP because of previous system limitations. The Agency will continue to work to improve processes in order to limit the need for this access. At the present time, the Information Technology Advisory Board (ITAB) has determined that it would not be cost effective to make significant changes to the EN Payment automation process. However, we are planning for an implementation to enhance EN Payments in Fiscal Year 2007. This will provide an opportunity to revisit the access issues presented in this recommendation.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Data Analysis and Technology Audits Division, (410) 965-9702

Albert Darago, Audit Manager, Application Controls Branch (410) 965-9710

Acknowledgments

In addition to those named above:

Anita McMillan, Auditor-in-Charge

Greg Thompson, Senior Auditor

Ron Anderson, Auditor

Cheryl Robinson, Writer/Editor

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 Specialist at (410) 965-3218. Refer to Common Identification Number A-14-05-15064.

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, Subcommittee on Human Resources

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

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

Chairman and Ranking Minority Member, Committee on Governmental Affairs

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

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

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

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

Chairman and Ranking Minority Member, Committee on Finance

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

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises 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 and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

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

Office of the Chief Counsel to the Inspector General

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

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.