OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

GENERAL CONTROLS REVIEW OF THE FLORIDA DIVISION OF DISABILITY DETERMINATIONS CLAIMS PROCESSING SYSTEM

January 2007 **A-14-06-16023**

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: January 10, 2007 Refer To:

To: Paul D. Barnes
Regional Commissioner
Atlanta

From: Inspector General

Subject: General Controls Review of the Florida Division of Disability Determinations Claims Processing System (A-14-06-16023)

OBJECTIVE

Our objective was to assess the general controls environment of the Florida Division of Disability Determinations (FL-DDD) claims processing system.

BACKGROUND

The Disability Insurance program provides benefits to wage earners and their families in the event the wage earner becomes disabled. The Supplemental Security Income program is a Federal income supplement program designed to help aged, blind, and/or disabled people who have little or no income. The Social Security Administration (SSA) implements the policies governing the development of disability claims under each program. Disability determinations under both programs are performed by an agency in each State or other responsible jurisdiction according to Federal regulations.[1] In carrying out its obligations, each responsible agency determines claimants' disabilities and ensures there is adequate evidence available to support its determinations.

Disability Determination Services' (DDS) personnel have access to extremely valuable and sensitive SSA data, such as Social Security numbers (SSN), medical information, and related disability claims data. Sensitive SSA data,[2] processed and stored by each DDS, should be protected from inappropriate or unauthorized access, use, and disclosure. DDSs have a responsibility to safeguard sensitive SSA data entrusted to them and to safeguard SSA's and DDS' systems accessed and used to process that data.

---

[1] 20 C.F.R., part 404, subpart Q, and part 416, subpart J.

[2] Sensitive data downloaded from SSA to the DDS claims processing system include claimant SSN, name, address, phone number and date of birth.

DDSs use a variety of hardware and software platforms to store, process, and protect sensitive SSA data. FL-DDD disability claims are processed on an IBM iSeries computer system (IBM computer) using I. Levy & Associates (iLevy), Inc. software.

The DDSs are expected to provide a control environment that meets SSA's minimum security requirements. SSA's security requirements for DDSs are found in its *Program Operations Manual System* (POMS).[3] The POMS provides SSA privacy and security program standards and guidelines, which apply to the DDS environment. SSA has also distributed Risk Models[4] to the DDSs to establish security settings for the various hardware platforms to help ensure the security of SSA data stored and processed on the DDS enterprise.

The FL-DDD maintains operations in six locations—Jacksonville, Miami, Orlando, Pensacola, Tallahassee and Tampa—and is a component of Florida's Department of Health. The IBM computer used by the FL-DDD to process claims is physically located at the Tallahassee location in the Ashley Building. Therefore, our physical security review was limited to the Ashley Building.

RESULTS OF REVIEW

We reviewed the general controls environment of the FL-DDD claims processing system and found it was generally in compliance with SSA standards. We found five physical security and four systems security-related issues that needed to be addressed to help ensure that SSA data stored and processed at the FL-DDD is secure. However, these issues do not rise to the level of impacting our overall conclusion.

We held an exit conference with the FL-DDD management as well as staff from the Atlanta Regional Office and SSA Headquarters to explain our findings and recommendations. The FL-DDD subsequently has addressed most of our findings. Although we did not independently review the newly implemented recommendations, we commend the FL-DDD on its efforts to help improve security.

PHYSICAL SECURITY ISSUES

Terminated and Transferred Employees Remained in the Physical Security Access Control System

We found six FL-DDD employees who had either been terminated or transferred during Fiscal Year (FY) 2006; however, active accounts for these employees still remained in the physical security access control system for the Ashley Building. Employees gain entry to the Ashley Building and interior passageways with an electronic key that is programmed with the employees' access requirements based upon their job duties. If

[3] POMS, Section DI 39566, *DDS Privacy and Security*.
[4] The Risk Model that was followed by the FL-DDD at the time of our review was the *iSeries Security Settings and Control Model* (commonly known as the *iSeries Risk Model*), October 2005.

an unauthorized individual has possession of one of these electronic keys and the account is still active in the physical security access control system, then that individual will have access to the building and interior passageways assigned to that key. SSA policy[5] states that office keys should be restricted to those individuals who are required to have them.

The physical security officer is responsible for administering physical access at the Ashley Building. However, there was no formal process to notify the physical security officer when an employee is terminated or transfers to another FL-DDD location. Systems access is removed via an automated request initiated by the employee's manager and is routed to the FL-DDD's systems Help Desk. The FL-DDD also uses an employee exit checklist whenever employees separate from or transfer to another location within the FL-DDD. This checklist details the items that the manager must collect prior to the employee's final day of work, such as access cards, building keys, and parking passes.

We recommended during our site visit that the automated Help Desk ticket and exit checklist processes be revised to incorporate the physical security officer so physical access will be removed for terminations and transfers to other FL-DDD locations. The FL-DDD stated that several processes have been implemented since our site visit to ensure the physical security officer is notified when an employee is being terminated or transferred. These processes are:

- The supervisor of an employee who is terminating or transferring to another location must notify the Ashley Building's physical security officer via email with the employee's name, access code number, and level of access.
- The physical security officer receives a weekly listing from the Human Resources (HR) Department of all employees who have separated from the FL-DDD.
- The employee exit checklist has been amended to include the physical security officer for the receipt of access cards, building keys, and parking passes.

The FL-DDD stated it will explore the feasibility of an automated procedure to notify the physical security officer of employee terminations and transfers as we had recommended. We encourage the FL-DDD to pursue implementing this automated process.

Employee Exit Checklists Were Not on File

Employee exit checklists for 27 of 75 terminated employees and 12 of 14 employees who transferred to other locations within the FL-DDD were not on file with the FL-DDD HR Department. Of the 50 exit checklists that were on file, 33 were not fully completed. Incomplete or missing checklists do not ensure that all FL-DDD property issued to terminated or transferred employees has been returned prior to their departure. SSA

[5] POMS, Section DI 39566.010 B.6.a., *DDS Physical Security.*

policy[6] states that personnel should turn in identification cards and all Agency property and that a copy of the completed checklist be maintained in the employee's personnel folder.

The checklist used by the FL-DDD directs the local offices to ensure that all fields on the form are addressed and that the completed checklist must be submitted to HR. We recommended at the exit conference that the FL-DDD issue a reminder to its field supervisors to ensure that all fields in the checklists are addressed and that completed exit checklists are submitted to the FL-DDD HR Department.

The FL-DDD stated that a process has now been implemented to ensure that exit checklists are completed and submitted to HR. Upon notification to HR that an employee is separating from or transferring to another location within the FL-DDD, the supervisor is sent the checklist and instructed to complete and submit the checklist to HR. The HR Department now monitors this process to ensure that checklists are completed and submitted by the supervisors. We commend the FL-DDD for its prompt action to correct this issue.

Excessive Personnel Had Access to the Computer Room

We found 5 out of the 31 employees who had been granted unescorted access to the Ashley Building's computer room had job duties not requiring them to have this access. These employees included administrative personnel, accounting personnel, and non-systems managers. This unescorted access would allow an employee, whether maliciously or accidentally, to damage FL-DDD equipment and data without FL-DDD systems or management staff's knowledge. SSA's POMS[7] states that access to the computer room should be restricted by management or authorized personnel. The Government Accountability Office's (GAO) *Federal Information Systems Controls Audit Manual* (FISCAM)[8] also recommends that access to an entity's computer room facilities and equipment should be limited to employees whose job duties and responsibilities require this access.

The physical security access codes that provide access to the Ashley Building's systems area office space also provides unescorted access to the computer room where the IBM computer is housed. While it may be necessary for some non-systems employees to have access to the systems area office space to meet with systems staff or to conduct other business, these employees should not have unescorted access to the computer room. We recommended at the exit conference the FL-DDD set up a separate access code for the computer room in its physical security access control system and that the systems area access of these employees be removed until separate access codes are in place for the systems office area and the computer room. The FL-DDD agreed with our recommendation. A separate access code has been implemented for non-systems employees that provides access to the systems office

[6] POMS, Section DI 39566.010 B.6.h., *DDS Physical Security*.
[7] POMS, Section DI 39566.010 B.2.l., *DDS Physical Security.*
[8] GAO FISCAM, January 1999, pages 46-47.

space but does not allow unescorted access to the computer room. Only employees whose job duties require unescorted access to the computer room have access now. We commend the FL-DDD for its prompt action to correct this issue.

Computer Room Housing the IBM Computer Did Not Have an Environmental Alarm System

The computer room in the Ashley Building, where the IBM computer is housed, did not have an environmental alarm system. Environmental controls can diminish the losses from some interruptions, such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied.[9] SSA policy[10] states that an environmental controls alarm system should be installed in DDS computer rooms.

The FL-DDD stated that it has determined its computer room environmental alarm needs and has requested funding from SSA. We recommend the FL-DDD continue to pursue the installation of an environmental control alarm system to prevent or mitigate damage within the computer room and interruptions in service.

Physical Security Weaknesses That Were Related to Door Construction

There were two doors with rising hinge pins on the ground level of the Ashley Building that lead from the public lobby (between 6 a.m. and 7 p.m.) into FL-DDD office space. Rising hinge pins can be tampered with and the door removed off of its frame. Also, the door leading into the systems office area did not have a peephole. Individuals ring a doorbell and verbally identify themselves to gain access to the systems office area.

SSA policy[11] states that perimeter doors should have non-rising hinge pins to prevent tampering with the hinges and should have peepholes if visibility is restricted. We recommended at the exit conference the FL-DDD install non-rising hinge pins or secure the existing hinges in a manner as to prevent the doors from being removed from their hinges. We also recommended a peephole be installed in the systems area office entrance door, so individuals without access to the area can be visually identified before being allowed to enter.

The FL-DDD agreed with our recommendations and stated that non-rising hinge pins have been installed on the two perimeter doors leading into its office space. The FL-DDD also stated a peephole has been installed in the systems area office entrance door. We commend the FL-DDD for its prompt action to correct these issues.

---

[9] GAO FISCAM, January 1999, page 128.
[10] POMS, Section DI 39566.010 B.2.m., *DDS Physical Security.*
[11] POMS, Section DI 39566.010 B.1.d. and 39566.010 B.1.e., *DDS Physical Security.*

SYSTEMS SECURITY ISSUES

Terminated Employees Still Had Enabled IBM Computer or Local Area Network Profiles

Two employees who were terminated during the current FY still had enabled IBM computer profiles at the time of our fieldwork. Also, another terminated employee had an enabled Windows local area network profile. Individuals whose profiles are enabled have the ability to sign-on to the system.

SSA provides the DDSs with the IBM computer Settings and Controls model (Risk Model) as a template for installation and management of the IBM computer platform. This document lists the required settings along with a risk description and underlying policy. The Risk Model states that accounts should be disabled immediately upon an employee's separation from duty.[12]

The process for disabling systems access for terminated employees at the FL-DDD is initiated by an automated Help Desk ticket request submitted by the employee's manager. If a Help Desk ticket request is not submitted, the terminated employee's account will remain enabled. Since our site visit, the FL-DDD issued a reminder to its area managers and bureau chiefs to follow the proper procedures for disabling terminated employees' systems access. We commend the FL-DDD for its prompt action to correct this issue.

Accounts Inactive for Over 30 Days Were Not Disabled

There were 24 user profiles not disabled after more than 30 days since their last date of access on the IBM computer. Also, there were six user profiles that had never signed onto the IBM computer for more than 30 days since the creation of the profiles and these profiles were not disabled. Inactive profiles increase the risk of inappropriate activity by unauthorized users. The risk of inappropriate activity is greater for profiles that have never signed onto the IBM computer because the FL-DDD uses a generic naming convention for its IBM computer profiles and a default password for initial sign-on.

SSA policy[13] states that accounts should be reviewed on a periodic basis and disabled after 30 days of inactivity. The FL-DDD agreed with our finding and stated a system job now runs weekly and disables profiles that have not signed onto the IBM computer in over 30 days or have not signed-on within 30 days of creation of the profile. We commend the FL-DDD on its prompt action to correct this issue.

---

[12] SSA's *iSeries Security Settings and Control Model,* October 2005, page 13.
[13] SSA's *iSeries Security Settings and Control Model,* October 2005, page 13.

IBM-Supplied Profile Not Configured in Accordance With Risk Model

We found an IBM-supplied profile on the IBM computer that was not configured in accordance with the SSA Risk Model. The IBM-supplied profile "QPGMR:"

- was used as a group profile for the FL-DDD programmers and batch users,
- was allowed to sign-on to the IBM computer, and
- had special authorities[14] assigned to it.

The SSA Risk Model[15] states that the QPGMR profile should not be used as a group profile and should not be allowed to sign onto the IBM computer. This ensures that individuals cannot sign onto the system under the group profile and perform activity that would not be attributable to those persons if they had signed onto the system under their individual user profile. The FL-DDD agreed with our finding and stated that the QPGMR profile can no longer sign onto the IBM computer. The FL-DDD is also coordinating with IBM and iLevy to develop a solution to no longer use QPGMR as a group profile.

The Risk Model[16] also states that the QPGMR should not have any special authorities assigned to it. However, the QPGMR profile is shipped from IBM with special authorities and IBM's Security Reference Manual for the IBM computer[17] cautions that removing special authorities from IBM-supplied profiles may cause system functions to fail. The FL-DDD has expressed concern that removing these special authorities may impact its production environment.

We recommend the FL-DDD continue to develop a solution enabling it to stop using the QPGMR profile as a group profile for the FL-DDD programmers and batch users. We also recommend the FL-DDD work with SSA to determine whether the special authorities can be removed from the QPGMR profile or whether the Risk Model requires revision.

---

[14] Special authorities are used to specify the types of actions a user can perform on system resources.
[15] SSA's *iSeries Security Settings and Control Model,* October 2005, page 9.
[16] *Id*.
[17] IBM, iSeries Security Reference Version 5 (SC41-5302-08), August 2005, page 271. The Security Reference Manual provides information about planning, setting up, managing, and auditing security on the iSeries system.

Restricted-Use Profiles Can Sign Onto the System

Six restricted-use profiles, which are vendor profiles and application group profiles, can sign onto the system in violation of SSA policy. SSA's Risk Model[18] states that these restricted-use profiles should not have the authority to sign onto the system. Profiles that are shared by groups or have widely known access rights and policies are subject to abuse and do not allow for accountability to a specific individual's actions.

We discussed this issue with the FL-DDD management at the exit conference conducted with staff from the Atlanta Regional Office and SSA Headquarters. These restricted-use profiles pertain to functions associated with the FL-DDD's iLevy software. Per consultations with iLevy, and by experimentation performed by the FL-DDD in its test environment, a determination has been reached that these restricted-use profiles must have the ability to sign onto the IBM computer. Restricting this ability would cause system functions to fail and impact production. The FL-DDD has shared these concerns with SSA and has decided not to change the restricted-use profile settings at this time.

The FL-DDD has worked with SSA and the Office of the Inspector General (OIG) to implement alternative security settings for these profiles. These security settings would offer an acceptable compensating control for being unable to prevent these profiles from signing on to the IBM computer as currently mandated by the SSA Risk Model. We recommend the FL-DDD continue to work with SSA to determine whether the Risk Model should be revised to reflect the production needs of the DDSs.

CONCLUSION AND RECOMMENDATIONS

We found the general controls environment for the claims processing system at the FL-DDD to be generally effective and in compliance with SSA policy. However, we identified physical and systems security areas where the FL-DDD could improve upon its protection of sensitive SSA data. We recommend the FL-DDD:

1. Pursue implementing an automated process to notify the physical security officer of employee terminations and transfers.

2. Continue to pursue the installation of an environmental control alarm system to prevent or mitigate damage within the computer room and interruptions in service.

3. Continue to develop a solution that enables termination of the QPGMR profile as a group profile for its programmers and batch users.

[18] SSA's *iSeries Security Settings and Control Model,* October 2005, page 14.

4. Continue to work with SSA to determine whether the special authorities can be removed from the QPGMR profile or whether the Risk Model requires revision.

5. Continue to work with SSA to determine whether the Risk Model needs revision to reflect the production needs of the DDSs.

AGENCY COMMENTS AND OIG RESPONSE

The Regional Commissioner essentially concurred with all five recommendations. Initially, the Regional Commissioner questioned the costs associated with recommendation 2 (see Appendix C). After further clarifying our position, the Regional Commissioner revised the comments and agreed to our second recommendation (see Appendix D).

For recommendation 4, the OIG asked that the Regional Commissioner to either modify the QPGMR profile or revise the Risk Model. The Regional Commissioner agreed to revise the Risk Model.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

C.F.R.	Code of Federal Regulations
DDS	Disability Determination Services
FISCAM	Federal Information System Controls Audit Manual
FL-DDD	Florida Division of Disability Determinations
FY	Fiscal Year
GAO	Government Accountability Office
HR	Human Resources
iLevy	I. Levy & Associates, Inc.
OIG	Office of the Inspector General
POMS	Program Operations Manual System
Risk Model	iSeries Settings and Controls Model
SSA	Social Security Administration
SSN	Social Security Number

Scope and Methodology

Our objective was to assess the general controls environment of the Florida Division of Disability Determinations (FL-DDD) claims processing system.

According to the Government Accountability Office (GAO),[1] general controls apply to all information systems—mainframe, minicomputer, network, and end-user environments. These controls include (1) entity-wide security program planning, management, [and] control over data center operations, (2) system software acquisition and maintenance, (3) access security, and (4) application system development and maintenance.

Our audit of the FL-DDD general controls consisted of (1) entity-wide security program planning, management and control over data center operations to include service continuity and environmental controls and (2) access security to include physical and system security. We did not review the FL-DDD system software acquisition and maintenance or application system development and maintenance.

To accomplish our objective, we:

- Reviewed the Social Security Administration's (SSA) security requirements sent to the Disability Determination Services, which included the Program Operations Manual System and the IBM iSeries computer system Security Settings and Control Model.
- Interviewed pertinent FL-DDD managers and personnel.
- Reviewed applicable guidance pertaining to the evaluation of general controls over computer-processed data from agency program information systems.
- Reviewed prior Office of the Inspector General reports and the PricewaterhouseCoopers LLP *Fiscal Year 2005 Management Letter* containing information relative to our objective.
- Obtained an understanding of the FL-DDD's general controls environment for its claims processing system and tested certain controls to determine whether they were effective and operating as intended.

We performed our field work at SSA Headquarters and at the FL-DDD Administrative Office in Tallahassee, Florida between March and May 2006. We conducted our review in accordance with generally accepted government auditing standards.

[1] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1, November 1999, page 16.

Agency Comments

SOCIAL SECURITY

Refer To: K. Killam 2-5727

MEMORANDUM

Date: November 28, 2006

To: Inspector General

From: Regional Commissioner
Atlanta

Subject: General Controls Review of the Florida Division of Disability Determinations Claims Processing System (A-14-06-16023)

Thank you for the opportunity to comment on the validity of the facts and reasonableness of the recommendations presented in your draft audit report of the Florida Division of Disability Determinations (FL DDD). We believe that the OIG Audit, regarding the general controls environment of the FL DDD claims processing system, was detailed and thorough.

Our response to the five recommendations is as follows:

1. **Recommendation: Pursue implementing an automated process to notify the physical security officer of employee terminations and transfers.**

   We agree with this recommendation. The OIG auditors found five physical security and four systems security-related issues that needed to be addressed within the FL DDD. The auditors recommended during their site visit that the automated Help Desk ticket and exit checklist processes be revised to incorporate the physical security officer. On April 21, 2006, the FL DDD implemented a change in procedure. The security liaisons for area offices are now notifying the Physical Security Coordinator of the name(s) and key number(s) of employees when they leave the FL DDD. The Physical Security Coordinator then updates the Master List of key holders. Therefore, physical access will be removed for all terminations and transfers to other FL DDD locations. Issue resolved and no further action is necessary.

2. **Recommendation: Continue to pursue the installation of an environmental control alarm system to prevent or mitigate damage within the computer room and interruptions in service.**

We do not agree with this recommendation. The auditors site our POMS DI 39566.010.B2 as the policy requirement for the installation of environmental controls in the computer rooms. The POMS policy states that this is a discretionary standard. The reference reads as follows: "We encourage DDS management to use the discretionary procedures to ensure ongoing security of data, personnel, and property. The DDS should consider, based on a risk assessment of their facilities (location, crime rate, current security level, etc.), whether some or all of the discretionary measures should be included in their security program. If a DDS is unable to meet a guideline for physical security, a risk assessment plan should be prepared." Based on the DDSs assessment of their security needs, SSA evaluates the value of funding these types of requests. SSA has determined that the cost of fire suppression systems far exceeds the value of the equipment and will not be funding the installation of environmental controls in the Florida DDD. Therefore, issue resolved and no further action is necessary.

3. **Recommendation: Continue to develop a solution that enables termination of the QPGMR profile as a group profile for its programmers and batch users.**

   We agree with this recommendation. The SSA Risk Model states that the QPGMR profile should not be used as a group profile and should not be allowed to sign onto IBM computers. The FL DDD agreed that individuals should not be able to sign onto the system under the group profile and perform activity that is not appropriate. Accordingly, the DDD began working with the iSeries Focus Group and SSA personnel in Central Office to resolve this issue with QPGMR. As a result, the QPGMR profile is disabled and initial program set to None for the FL DDD iSeries. Therefore, users cannot log on to the FL DDS iSeries using QPGMR. Issue resolved and no further action is necessary.

4. **Recommendation: Continue to work with SSA to determine whether the special authorities can be removed from the QPGMR profile or whether the Risk Model requires revision.**

   We do not agree with the recommendation of removing the special authorities from the QPGMR profile, but believe that the Risk Model should be revised. The Risk Model states that the QPGMR should not have any special authorities assigned to it. The FL DDD was concerned, however, that removing special authorities might impact their production environment. Since the initial findings by the auditors, SSA personnel in Central Office have revised the Risk Model. The Risk Model now indicates that QPGMR is shipped by IBM with special authorities and that they should not inherently indicate a security issue. Therefore, all DDSs (including the FL DDD) can continue to utilize the QPGMR profile as needed by the application vendors (i.e. Levy, Versa and Midas), but should not add any additional special authorities to the QPGMR profile that are not already present. The FL DDD and SSA will continue to take care that QPGMR profile is utilized correctly.

5. Continue to work with SSA to determine whether the Risk Model needs revision to reflect the production needs of the FL DDD.

We agree with this recommendation. Auditors found six restricted-use profiles, which are vendor profiles and application group profiles that could sign onto the system in violation SSA policy. SSA's Risk Model states that these restricted-use profiles should not have the authority to sign onto the system. Profiles that are shared by groups or have widely known access rights and policies are subject to abuse and do not allow for accountability to a specific individual's actions. Therefore, FL DDD has reminded area managers and bureau chiefs to follow procedures for disabling employee's systems access (as outlined above). The FL DDD and SSA will continue to monitor these procedures to ensure compliance by area manages and bureau chiefs. The Quarterly Security review of all systems access accounts will ensure any deficiency is found and corrected.

Your staff may direct questions to Josie Irwin at (404) 562-1407 or Karen Killam at (404) 562-5727.

Paul D. Barnes

cc: James McHargue
Paul Buehler
Josie Irwin

Agency Comments - Revised

SOCIAL SECURITY

Refer To: K. Killam 2-5727

MEMORANDUM

Date: December 19, 2006

To: Inspector General

From: Regional Commissioner
Atlanta

Subject: General Controls Review of the Florida Division of Disability Determinations Claims Processing System (A-14-06-16023) – Revision

We responded to the above draft audit report on November 28, 2006. Our response to the 2nd recommendation regarding the installation of an environmental control alarm system indicated that we did not agree with the recommendation. Our response dealt with the installation of an environmental suppression system, which we believed was not cost effective. However, in the interim, we realized that OIG was recommending the installation of an environmental control system and not a suppression system.

Our updated response is as follows:

2. **Recommendation: Continue to pursue the installation of an environmental control alarm system to prevent or mitigate damage within the computer room and interruptions in service.**

We agree with this recommendation. We are requesting funding for the installation of an environmental control alarm system to prevent or mitigate damage within the computer room. The Regional Office will work with the Florida DDS to ensure that this system is purchased and installed this fiscal year. Issue is on-going until the control alarm system is installed.

Your staff may direct questions to Josie Irwin at (404) 562-1407 or Karen Killam at (404) 562-5727.

Paul D. Barnes

cc: James McHargue
Paul Buehler
Josie Irwin

OIG Contacts and Staff Acknowledgments

OIG Contacts

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

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

Acknowledgments

In addition to those named above:

Alan Lang, Senior Auditor

Annette DeRito, 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-14-06-16023.

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.