OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

SINGLE AUDIT OF THE
COMMONWEALTH OF VIRGINIA
FOR THE FISCAL YEAR ENDED
JUNE 30, 2007

December 2008 **A-77-09-00005**

MANAGEMENT ADVISORY 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: December 18, 2008 Refer To:

To: Candace Skurnik
Director
Audit Management and Liaison Staff

From: Inspector General

Subject: Management Advisory Report: Single Audit of the Commonwealth of Virginia for the Fiscal Year Ended June 30, 2007 (A-77-09-00005)

This report presents the Social Security Administration's (SSA) portion of the single audit of the Commonwealth of Virginia for the Fiscal Year (FY) ended June 30, 2007. Our objective was to report internal control weaknesses, noncompliance issues, and unallowable costs identified in the single audit to SSA for resolution action.

The Auditor of Public Accounts performed the audit. We have not received the results of the desk review conducted by the Department of Health and Human Services (HHS). We will notify you when the results are received if HHS determines the audit did not meet Federal requirements. In reporting the results of the single audit, we relied entirely on the internal control and compliance work performed by the Auditor for Public Accounts, and the reviews performed by HHS. We conducted our review in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

For single audit purposes, the Office of Management and Budget (OMB) assigns Federal programs a Catalog of Federal Domestic Assistance (CFDA) number. SSA's Disability Insurance (DI) and Supplemental Security Income (SSI) programs are identified by CFDA number 96. SSA is responsible for resolving single audit findings reported under this CFDA number.

The Virginia Disability Determination Services (DDS) performs disability determinations under SSA's DI and SSI programs in accordance with Federal regulations. The Virginia DDS is reimbursed for 100 percent of allowable costs. The Department of Rehabilitative Services (DRS) is the Virginia DDS' parent agency.

The single audit reported that:

1. DRS does not provide employees training on information security. The corrective action plan indicated that DRS is in the process of updating its Security Awareness Training Program to include information security as well as physical security (Attachment A, page 1).

2. DRS data exchanged between two computer systems was not adequately protected (e.g., encrypted). The corrective action plan indicated that DRS is working with SSA to correct the deficiency (Attachment A, pages 1 and 2).

3. One DRS employee had the dual ability to create and approve payroll transactions. The corrective action plan indicated that DRS will remove this employee's ability to both create and approve transactions (Attachment A, page 3).

We recommend SSA:

1. Ensure DRS developed training that addressed information security.

2. Verify that controls have been put in place to protect DDS data exchanged between computer systems.

3. Confirm that DRS terminated the employee's ability to create and approve payroll transactions.

The single audit also identified concerns related to policies and procedures applicable to DRS' network administration and configuration; system and backup monitoring; and access and password controls (Attachment B). Although this finding was not specifically identified to SSA, it may have an impact on DDS operations. I am bringing this matter to your attention as it represents a potentially serious computer control problem for the Agency.

Please send copies of the final Audit Clearance Document to Shannon Agee. If you have questions contact Shannon Agee at (816) 936-5590.

Patrick P. O'Carroll, Jr.

Attachments

SOCIAL SECURITY ADMINISTRATION

Other Internal Control Findings

07-47 Update and Expand Security Awareness Training

Applicable to: Department of Rehabilitative Services

Rehabilitative Services should update its Security Awareness Training and provide system users with regular training to minimize the risks of not maintaining the confidentiality, integrity, and availability of information. Rehabilitative Services operates a Security Awareness Training program that does not address the risks of protecting the department's data. Additionally, Rehabilitative Services does not require users to receive regular refresher training to update their Security Awareness. Updates help ensure that users are aware of new policies, procedures, or risks to Rehabilitative Services' information.

Rehabilitative Services should evaluate and update the content of its Security Awareness Training and develop a process for providing system users with regular refreshers courses. Rehabilitative Services should annually review the content of its Security Awareness Training to ensure it addresses any new risks.

Management Plan for Corrective Action

The Department of Rehabilitative Services concurs with this recommendation and is in the process of updating its Security Awareness Training Program. The training will include, but not be limited to, protecting the Disability Service Agencies' data and minimizing risks associated with issues confidentiality, integrity, and availability of information. The training will address Information Technology Security as well as physical security.

The Department of Human Resource Management's (DHRM) Knowledge Center will be used to track employee's completion of the Security Awareness Training. The system will be used as a tool to ensure that employees are provided both the initial training as well as periodic refresher training.

Responsible Party: John Payne, Security Officer

Estimated Completion Date: June 30, 2008

07-48 Improve Data Protection

Applicable to: Department of Rehabilitative Services

Rehabilitative Services exchanges data between two systems that do not adequately protect the data. Inadequate data protection of Rehabilitative Services' mission critical data places the confidentiality, integrity, and availability of the Commonwealth's information at risk. The Commonwealth's information security standards require that agencies encrypt data before the transmission of sensitive information in order to minimize the risk of compromising the sensitive data.

Rehabilitative Services should apply the Commonwealth's information security standards consistently to all applications housing sensitive and mission critical information. Rehabilitative Services should start this process by dedicating the necessary resources to review and remediate the risks to their sensitive and mission critical applications.

Management Plan for Corrective Action

While the Department of Rehabilitative Services (DRS) concurs with the findings of the APA, it should be noted that the Federal Department of Social Security Administration mandates that DRS uses the (Virginia) Claims Processing System. This system is subject to Federal security standards. We are in contact with our Federal partners and all parties are currently working diligently to correct this system deficiency. The Agency (DRS) expects to have this issue resolved by use of secure File Transfer Protocol (FTP) no later than March 31, 2008. The Department of Rehabilitative Services will also systematically review other FTP scripts to be sure this issue does not occur with other data interfaces in the future.

Responsible Party: John Payne, Security Officer

Estimated Completion Date: March 31, 2008

07-49 Remove an Employee's Ability to Create and Approve Payroll Payments

Applicable to: Department of Rehabilitative Services

An employee at Rehabilitative Services has the ability to create and approve payroll payments. At Rehabilitative Services' recommendation, the Department of Accounts (Accounts) granted this employee two separate passkeys to the CIPPS. The combination of functions associated with these passkeys allows this employee to circumvent the controls designed into CIPPS.

Rehabilitative Services processes payroll for all six Disability Service Agencies. This employee has the ability to create and approve payroll payments for all six agencies. Rehabilitative Service's payroll staff averages between three and four employees and processes payroll for about 1,700 employees. Currently, Rehabilitative Services' policy of not allowing this individual to create and approve the payroll payments for the same agency is the only control limiting their functionality.

Rehabilitative Services and Accounts should consider the risk of allowing one employee both types of access, and should consider removing one of their access types.

Management Plan for Corrective Action

As noted in the APA finding, the Department of Accounts granted this dual CIPPS access type based on the volume and number of agencies served by DRS and the limited number of Payroll staff to do the job. DRS concurs that an internal control risk exists because of this dual CIPPS access type; however, controls were put in place to mitigate this risk. At no time did the employee in question certify and release any payroll that they had been responsible for processing or keying. System controls were put in place to ensure that did not occur. With the recent hire of an additional Payroll Accountant position in the DRS Payroll Unit, the need for a position to maintain dual CIPPS access types diminished. Therefore, effective on or before March 10, 2008, the employees in question will no longer have dual access to CIPPS. This action should effectively mitigate any unnecessary risk in the Payroll area.

Responsible Party: Phil Benton, Fiscal Director

Estimated Completion Date: March 10, 2008

RISK ALERT

During the course of our audits, we encounter issues that are beyond the corrective action of management and require the action of wither another agency, outside party, or the method by which the Commonwealth conducts its operations.

Security Risk Assurance for Infrastructure

Applicable to: *Department of Taxation, Department of Social Services, Department of Mental Health, Mental Retardation, and Substance Abuse Services, Department of Health, Department of Rehabilitative Services, and Department of Alcohol Beverage Control (The Departments)*

The Departments above have responsibility for the security and safeguarding of all of its information technology systems and information. Over the past four years, the Commonwealth has moved the information technology infrastructure supporting these systems and the information they contain to the Virginia Information Technologies Agency (VITA), who has an Information Technology Partnership (IT Partnership) with Northrop Grumman. In this environment, VITA and each Department clearly share responsibility for the security of each Department's information technology assets, systems, and information and must provide mutual assurance of this safeguarding.

The Departments have provided VITA with all the documentation required to make this assessment and VITA should provide assurance that the IT Partnership will practice proper policies and procedures as outlined by each Department. VITA had a special audit done of the IT Partnership and will communicate any findings and corrective action to the Departments.

The special audit identified that the IT Partnership:

- Had no formal, documented policies and procedures for network administration and configuration, system monitoring, and backup monitoring and error resolution; and
- Had weak access and password controls for Windows domain servers.

Documented policies and procedures and strong access and password controls are critical in order to minimize the security risks relating to the confidentiality, integrity, and availability of the Departments' information stored on the IT Partnership's hardware and infrastructure.

Although the Departments are not responsible for correcting these findings, they should receive regular status reports from VITA on the progress the IT Partnership is making to correct the issues. As part of the progress reporting, VITA should provide the Departments with any interim steps they should take if the IT Partnership must delay addressing this issue. We bring this matter to the attention of the Departments, so that they can properly manage their risk and monitor corrective action.

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.