SOCIAL SECURITY

MEMORANDUM

Date: March 10, 2004 Refer To:

To: Martin H. Gerry
Deputy Commissioner
for Disability and Income Security Programs

From: Assistant Inspector General
Audit

Subject: Evaluation of the Accelerated eDib System – Fifth Assessment (A-14-04-14057)

The Social Security Administration's (SSA) Office of the Inspector General (OIG) has completed its fifth assessment in our ongoing evaluation of the Accelerated eDib (AeDib) initiative (formally the Electronic Disability or eDib initiative). We conducted this fifth assessment from August 2003 through March 2004 at SSA Headquarters in Baltimore, Maryland. While we did not conduct an audit of the AeDib process, our assessment addressed those issues that arose at the AeDib Steering Committee, or where we were asked to provide comments to the Office of Systems.

BACKGROUND

As part of our participation in the Accelerated eDib (AeDib) Steering Committee and prior evaluations[1] of the AeDib project we recommended that the Agency conduct a risk assessment of the AeDib system. The Clinger-Cohen Act of 1996 (CCA)[2] requires proposed IT projects be qualitatively and quantitatively assessed for risk and return. The Office of Management and Budget (OMB) also requires Federal agencies to consider risk when deciding what security controls to implement.[3] OMB requires a risk-based approach to determine adequate security, and it encourages agencies to consider major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

[1] *Assessment of the Electronic Disability Project's Pre-2005 Business Process*, (A-14-02-22066) February 26, 2002, and *Evaluation of the Accelerated eDib System Third Assessment*, (A-14-03-13047) December 20, 2002.

[2] Sections 5122(a), 5122(b)(3), and 5122(b)(5) of the CCA, Pub. L. No. 104-106 §§ 5122(a), 5122(b)(3), 5122(b)(5), 110 Stat. 186, 683 (1996).

[3] OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, page 8.

The National Institute of Standards and Technology (NIST) also recognizes the importance of conducting risk assessments for securing computer-based resources. A security risk assessment enables management to make informed risk-based business decisions.

The purposes of our fifth assessment of AeDib were to: (1) evaluate the five risk assessments issued by the Agency in July 2003; and (2) determine whether the Agency should perform a Post-Implementation Review of AeDib before the scheduled national roll-out. The OIG had earlier called for these risk assessments, first at the AeDib Steering Committee meetings and later, formally, in its third AeDib assessment. We were asked by the Office of Systems to evaluate the Agency's risk assessments for AeDib. We reported our findings separately to the Office of Systems, which has already taken action to improve these assessments.

RESULTS OF OUR EVALUATION OF THE FIVE AeDib RISK ASSESSMENTS

The five risk assessments for which the Agency received contractor assistance to complete and then requested the OIG to evaluate are as follows:

1. The Electronic Disability Collection System.
2. The Document Management Architecture.
3. AeDib Internet Applications.
4. The Office of Hearings and Appeals Case Processing and Management System.
5. The Disability Determination Services (DDS) AS/400.

The first four assessments were performed to address the risks to the major AeDib software subsystems (See Table 1 in Attachment A for a summary of the software related recommendations), while the fifth addressed the hardware system that supports the disability claims processing software used by the DDSs in the 50 States and 4 other jurisdictions (See Table 2 in Attachment B for a summary of the AS/400 related recommendations).

We found that the text supporting the security plan recommendations in all four software risk assessments used general support system terminology instead of major application terminology. Additionally, the Agency agreed with our conclusion that the four software risk assessments should be updated. We found that SSA had already begun addressing the issues the contractor raised about the AS/400. We recommend that the Agency amend the text supporting the security plan recommendations and update the four software risk assessments. We recommend the Agency have its contractor review the pertinent control documents that SSA recently issued and update the AS/400 assessment. We also recommend the Agency conduct Post-Implementation Reviews of each AeDib software subsystem during Fiscal Year 2005.

Four Risk Assessment Recommendations Caused Delays

SSA issued four risk assessments of the Agency's AeDib software systems containing recommendations using the terminology of OMB's general support system[4] (GSS) criteria. However, the Agency did not determine that all four software systems met OMB's definition of a major application[5] (MA) until after the risk assessments were issued in July 2003. As a result, the recommendations in the risk assessment did not call for: (1) preparation of an Application Security Plan; and (2) conducting a review of the application controls of these four systems. Shortly after we met with the Agency on October 7, 2003, we brought up the MA issue and the Agency took immediate action to begin implementing the two remaining recommendations. The Agency completed the Application Security Plans in December 2003 and expects to complete the review of the application controls of the four systems by March 2004.

The Four Software Risk Assessments Needed Updating

We found that each risk assessment needed updating. In each of the four risk assessments, SSA issued a set of five virtually identical recommendations. Appendix B in all four software risk assessments did not cite any evidentiary support for 4 of the 5 recommendations made by the Agency. For the remaining recommendation in 2 of the applications, Appendix B did cite evidentiary support for 6 of the 10 items reviewed, but did not cite any support for the 10 conclusions in the other 2 applications.

Averaging the results of the four risk assessments, each risk assessment concluded that the Agency did not plan to implement key security requirements even though about 40 percent of the requirements (39 of 98) designated by SSA as "Not Planned for Implementation" were required by the Agency's Information System Security Handbook (Handbook). However, we were assured by Agency officials that the risk assessments simply needed updating and that SSA would in fact implement the requirements called for by the Agency's Handbook.

[4] A "general support system" or "system" means an interconnected set of information resources under the same direct management control, which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, and a departmental data processing center including its operating system and utilities. OMB Circular No. A-130, Appendix III, section A.2.c.

[5] A "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. Source OMB Circular No. A-130, Appendix III, section A.2.d.

The Disability Determination Services IBM AS/400 Risk Assessment

In July 2003, SSA released a risk assessment that addressed the adequacy of the management, operational and technical security controls in place to secure the DDS AS/400 environment that resides within each DDS. The document identified two issues detailed in Table 2 in Attachment B, relating to the DDS AS/400, and recommended the development of: (1) a System Security Plan for the AS/400 system; and (2) a formal certification and accreditation process.

However, prior to the release of the risk assessment, the Agency's existing guidance already addressed these two issues and provided management with the operational and technical security controls that DDSs should implement to protect sensitive SSA data. The guidance is located in SSA's DDS Security Document and risk model for AS/400s. Therefore, SSA should have provided its contractor with these documents so that the contractor could have reviewed the adequacy of SSA's existing guidance, and assessed how this guidance could be used to mitigate risks for the DDS AS/400s.

While SSA's recent requirements for the DDSs are a major step to address the security needs at the DDSs, the DDSs still need to enact the Agency's requirements to make them effective. Therefore, once the DDSs implement these new requirements, the security of SSA's data should be greatly enhanced. Furthermore, security at the DDSs will take on increased importance in 2004, when SSA begins granting the DDSs direct access to the Agency's electronic folder. Since the electronic folder will contain sensitive medical, claim and identity information, someone gaining improper access through a DDS could obtain access to the Agency's data.

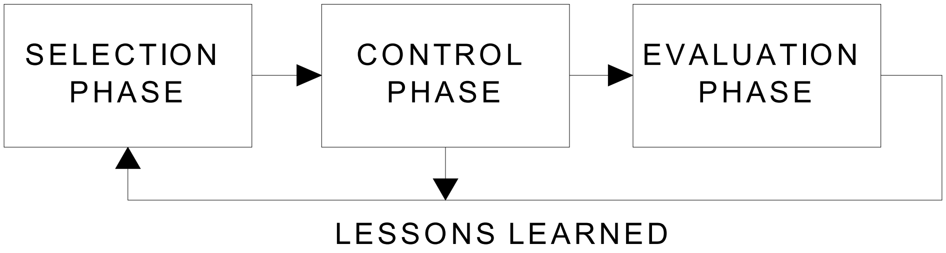
SSA Should Perform a Post-Implementation Review of the Agency's New Electronic Disability Process Before the National Roll-Out is Completed

We believe the current Electronic Disability System is being implemented in a more efficient manner than the two previous electronic disability projects.[6] One reason for improvement during this most recent project is because the Agency conducted a post-implementation review of the prior application. The post-implementation review helped the Agency assess why the previous systems had to be redirected, costing SSA about $70 million.[7] Office of Systems officials told us that they plan to do a post-implementation review before the national roll-out of the AeDib software is complete.

[6] SSA initiated the Modernized Disability System to redesign the disability claims process in 1992. The project was redesignated the Reengineered Disability System in 1994.

[7] *Information Technology Capital Planning and Investment Control Process at the Social Security Administration*, (A-14-99-12004) March 30, 2001, page D-2.

In February 1997, the General Accounting Office (GAO) issued guidance[8] to all Executive Branch agencies for evaluating IT investment decision making for implementing the Clinger-Cohen Act of 1996 (CCA) and other major legislation. While SSA is not required to adopt this guidance, the Federal Chief Information Officer Council has endorsed this guidance as "best practices" for implementing CCA. The guidance provides a three-phase process (Selection, Control, and Evaluation) for capital planning and IT investments (see graphic of process below).



The Evaluation phase "closes the loop" on the IT investment management process by conducting post-implementation reviews. Post-Implementation reviews identify areas where future decision making can be enhanced. Lessons learned during the evaluation phase should be geared toward modifying future selection and control decisions. Valuable lessons learned can be incorporated into the Selection and Control phases to help minimize risk and maximize benefits on future IT projects. We highly suggest that the Agency should perform a post-implementation review during Fiscal Year 2005. Finally, the Agency needs to incorporate its new electronic disability system into its Federal Managers' Financial Integrity Act reviews that it contracts-out for audit.

[8] *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*, GAO/AIMD-10.1.13, February 1997.

There is no expectation for the Agency to formally respond to this document. If you have any questions or comments, please call me or have your staff contact Kitt Winter, Director, Data Analysis and Technology Audit Division at (410) 965-9702, or Al Darago at (410) 965-9710.

Steven L Schaeffer

Steven L. Schaeffer

Attachments

cc:
Chief Information Officer
Deputy Commissioner for Systems
Deputy Commissioner for Operations
Acting Inspector General
Assistant Deputy Commissioner for
Disability and Income Security Programs
Associate Commissioners for
Disability Programs
Chair AeDib Steering Committee
Director, Audit Management and Liaison Staff

Attachment A

Table 1: Findings for the Four Software Risk Assessments

Number	Risk Level	BLSR No.	Finding Description	Recommendation
Management Control				
6.1.1.1	***Medium***	MC1.1-1.8	A System Security Plan (SSP) has not been completed and approved for all four software components of AeDib.	To comply with the requirements of OMB A-130, SSA should develop a SSP for all four software components of AeDib.
6.1.1.2	***Medium***	MC3.1-3.10	Security controls need to be reviewed on a periodic basis.	The security controls for all four software components should be reviewed a minimum of once every 3 years or whenever any of the four application conditions change.
6.1.1.3	***Medium***	MC5.1-5.16	A formal system Certification and Accreditation (C&A) needs to be completed for AeDib.	A formal C&A process should be completed for AeDib to ensure that all security controls are implemented.
Operational Control				
6.1.2.1	***High***	OC1.1-1.43	A contingency plan or continuity of operations plan (COOP) needs to be completed for all four software components of AeDib.	Complete a contingency plan and COOP for all four software components of AeDib. The plan should include preparations for maintaining all four software components of AeDib in the event of a disaster.
6.1.2.2 **(DMA only finding)**	***Medium***	OC2.1-2.3	A formal documented configuration management process (CMP) needs to be in place for new or revised hardware/software testing, upgrades, and modifications.	A formal CMP should be developed to prevent possible loss of data and resources on the Document Management Architecture (DMA) system.
Technical Control				
6.1.3.1	***High***	TC3.1-3.21 MC3.1	Auditing functionality for all four software components of AeDib requires more detailed development of audit requirements.	Auditing must be configured to capture security events such as date and time of the event, applicant associated with the event, type of event, actions performed, system resources accessed, and the success or failure of the event. In addition, the audit trail should provide information about the originator of electronic transactions (i.e., sending location, sending entity) and other measures to ensure the integrity of the document.

Attachment B

Table 2: DDS AS/400 Findings

Number	Risk Level	BLSR No.	Finding Description	Recommendation
Management Control				
6.1.1.1	***Medium***	MC2.1-2.8	A System Security Plan (SSP) has not been completed and approved for the DDS AS/400.	To comply with the requirements of OMB A-130, SSA should develop a SSP for the DDS AS/400.
6.1.1.2	***Medium***	MC7.1-7.16	A formal system Certification and Accreditation (C&A) needs to be completed for AeDib.	A formal C&A process should be completed for AeDib to ensure that all security controls are implemented.