# SOCIAL SECURITY

**MEMORANDUM**

Date: December 20, 2002 Refer To:

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

From: Assistant Inspector General
for Audit

Subject: Evaluation of the Accelerated eDib System – Third Assessment (A-14-03-13047)

The Social Security Administration's (SSA) Office of the Inspector General (OIG), has completed its third assessment in our on-going evaluation of the Accelerated eDib (AeDib) system (formerly the Electronic Disability or eDib) system. We provided many of our ideas and concerns during the eDib planning process through participation in the AeDib Steering Committee.

As part of the assessment, we considered the following issues:

- The eDib's Program Management Plans and Risk Management Plans.
- The AeDib cost benefit analysis (CBA).
- Oversight of the AeDib System by its Steering Committee.
- The AeDib Project Plan.
- The Project Scope Agreement (PSA) for Enterprise Document and Imaging Management Architecture (EDIMA) for the AeDib Project.
- The internal controls necessary in scanning hardcopy disability evidence at remote sites.

**The eDib Program Management Plans and Risk Management Plans**

During the October 2, 2001, meeting of the eDib Steering Committee, OIG expressed concern that the *eDib Program Management Plan* dated August 3, 2000, neither addressed security nor evaluated the risks involved in eDib program development. OIG's concerns were partially addressed in the November 14, 2001, *eDib Program Management Plan*.

However, the plan did not address the risks associated with security, fraud, hackers and complexity of the system. Instead, the Risk Management Plan addressed development risks, which could be incurred during systems development, such as cost, schedule, integration/technical and mission. While system development risks should be considered, it is as important to address risks that relate to internal controls and security.

SSA added the OIG's recommendations to address internal controls and added risks associated with fraud, hackers and complexity of the system to its January 31, 2002, *eDib Program Management Plan* (See Attachment A*).* However, the Booz Allen Hamilton contract only required conducting a process risk assessment, which would evaluate risks such as the ability to deliver the AeDib system on a timely basis.

OIG informed the AeDib Steering Committee about the necessity of conducting a security risk assessment. For the fiscal year ending September 30, 2001, SSA processed an average of 2.2 million initial disability benefits. For a system that is so important to so many Americans, a security risk assessment, during the early stages of systems development, should be both cost effective and essential. A security risk assessment would help ensure that a fully operational AeDib System will operate with an appropriate level of controls to help prevent fraudulent transactions and minimize risk. A security risk assessment is also required during system development by the Office of Management and Budget (OMB),[1] which utilizes guidelines issued by the National Institute of Standards and Technology (NIST),[2] and also by SSA's own Project Resource Guide (PRIDE).[3]

At the December 17, 2002, AeDib Steering Committee, it was announced that based on the recommendations of our OIG, the Agency will be conducting a risk assessment of the AeDib system.

### The AeDib Cost Benefit Analysis

At the request of SSA, OIG reviewed the AeDib CBA. OIG only reviewed the CBA for its overall content. We believe the CBA is unclear on how SSA obtained and verified the project's costs and processing times (See Attachment B). For example, we saw no evidence that the Electronic Disability Collection System's costs were verified; yet these costs and the corresponding projected savings are major factors in the AeDib project. Furthermore, the costs to store the back-up of electronic data are excluded from the CBA. The storing of back-up data could also be a substantial cost of the project with up to 270 pages of scanned data for each claimant in addition to the backup of initial and post-entitlement claims information.

[1] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, p. 7.

[2] NIST Special Publication 800-12, *An Introduction to Computer Security*, section 7.1, p. 59.

[3] PRIDE, Security Processes, Security Task Definitions, page 2.

## Oversight of the AeDib System by its Steering Committee

The AeDib Steering Committee and the Associate Commissioners Electronic Service Delivery Steering Committee need more oversight of AeDib. A number of AeDib Steering Committee meetings have been cancelled; for example, the Committee had only one meeting from June 4, 2002 through August 26, 2002. Since SSA accelerated the completion time for the AeDib system to January 2004, we believe it is essential the Steering Committee meet on a regular basis. We informed the then Chairperson of the Committee of our concern, and as a result, the AeDib Steering Committee has resumed meeting on a regular basis.

## The AeDib Project Plan

The initial AeDib project plan projected the start and stop dates for systems work (see Attachment C) but did not include times necessary for important deliverables such as functional requirements or systems security that should be in place before the system goes into production. We informed the Committee of our concerns, and the appropriate staff took immediate action to issue a revised project plan for the AeDib system, which included the additional dates.

## Project Scope Agreement for Enterprise Document and Imaging Management Architecture for the AeDib Project

The PSA provides a timeline for the completion of scanning paper documents into the AeDib System. The Office of Systems sent this document to other Agency components for comment. The OIG had numerous concerns regarding deferring the full implementation of the security/internal controls (see Attachment D). The document proposed deferring such basic and essential controls as an automated audit trail and the ability to “lock” a document to prevent further inappropriate annotation or modification to that document. Numerous SSA components agreed that the system should not be placed into production without at least basic internal controls. Because of these comments, the Committee reassessed the need for internal controls in the system. As a result, the Agency worked with a contractor and enhanced controls in its EDIMA System for the AeDib Project. OIG, however, still expressed reservations primarily concerning the possible implementation of controls without benefit of the required risk assessment and plans the Agency may have to eliminate the wet signature, without compensating controls.

However, the December 5, 2002, EDIMA requirements no longer called for the destruction of paper documents. As mentioned above, at the December 17, 2002 AeDib Steering Committee, it was announced that based on the recommendations of the OIG, the Agency will include a risk assessment of EDIMA in its overall risk assessment of the AeDib system.

## Internal Controls Necessary in Scanning of Hardcopy Disability Evidence at Remote Sites

The AeDib CBA calls for the Agency to contract out the scanning of hardcopy disability documents received into the electronic folder as part of its disability process. If SSA contracts out the scanning of hardcopy disability documents, the Agency will need sufficient procedures to establish that the scanned evidence was reliable. The following are important considerations needed when contracting out the scanning of hardcopy disability documents:

- A protocol is necessary to ensure procedures are consistently applied at every processing site.
- If litigation occurs, the Agency might need an expert who could testify as to how the process works and why it is reliable.
- Once the contractor captures the record, there should be controls in place to limit alteration of the record.
- There should be a record of the person capturing the form, which also shows how the record was received and on which date. There should be an audit trail to trace any later changes to the document.
- The medium on which the contractor retains the form should be secure yet easily accessible to SSA. The contractor should back up the information.
- The contractor should fully understand legal privacy protections afforded this information. The contract should specify responsibilities, liabilities and recourse.
- The contractor should capture the documents in their entirety. Paper copies should be retained whenever there is suspected fraud.[4]

Should the Agency decide to perform the scanning function in-house, many of these same procedures will still apply to the electronic process.

[4] While the extent of internal controls should be risk-based, the Agency should maintain, at a minimum, a system sufficiently reliable to successfully prosecute those who commit fraudulent acts against SSA's programs. Doing otherwise puts at-risk the Agency's assertion that its internal controls are adequate and whether SSA will continue to receive an unqualified opinion on its financial statements. The maintenance of an adequate internal control process is essential if the Agency is to remove the information protection reportable condition on its financial statements and the General Accounting Office's designation of the title XVI program as high-risk.

We believe this assessment will assist the Agency to enhance the eDib systems development process. We gathered our information in Baltimore, Maryland. There is no expectation for the Agency to formally respond to this document. We look forward to our future participation in the AeDib Steering Committee. 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:
Inspector General
Chair, AeDib Steering Committee
Candace Skurnik, Acting Director
Management Analysis and Audit Program Support Staff

December 13, 2001

NOTE TO: Nancy Webb

SUBJECT: Comments on the Booz Allen & Hamilton *eDib Program Management Plan*

We believe that the Booz Allen & Hamilton November 30, 2001, *eDib Management Plan* is much improved over the initial Management Plans and addresses many of our prior comments made to the Office of Disability. Specifically, it includes a risk assessment, key initiative and a Disability Case Intake Process Plan. While much is still left unanswered until the project moves further along, it appears that internal controls and security will be addressed.

We will continue to work with the eDib Steering Committee on the Management Plan, which is described as a "living document." One of our main concerns is that the eDib Risk Management Plan stresses managerial risks associated with completing the project and does not address the risks in the eDib system not possessing adequate internal controls. Appendix H titled the "Disability Case Intake Process Plan," however, does call for a technical risk assessment throughout the eDib process including in the requirements phase. We will reevaluate the proposed internal controls in the eDib System once all of the planning documents are completed and again at the requirements phase of the process. As we have stated in the past, the eDib system needs to have adequate internal controls and security over information, especially with respect to establishing compensating controls, such as an audit trail, along with any plans to eliminate the "wet signature" from the application process. Elimination of any of the current internal controls and implementation of any new controls needs to be based on a comprehensive risk assessment.

We prepared these suggestions to help facilitate the eDib systems development process. There is no expectation for the Agency to formally respond to these suggestions. We look forward to working with SSA as the eDib system is implemented. If you have any questions or comments, please call me or have your staff contact Kitt Winter, Director, Systems Audit Division at (410) 965-9702.

*Steven L. Schaeffer*

## Office of the Inspector General
## Comments on the Booz, Allen & Hamilton eDib Program Management Plan

| PAGE | COMMENTS |
|---|---|
| ES-3 | Consider adding the issue of Public Key Infrastructure and electronic signature as one of the projects under the eDib Delivery Strategy |
| II-7 | Under business needs we should include the ability to prosecute offenders, and material sufficient for appeals to OHA |
| V-7 | Under the Quality Assurance and Evaluation we should include a post-implementation review as called for under the Clinger-Cohen Act. |
| Appendix A | Include the risk assessment as a separate task |
| Appendix C | The issue of developing and placing of information management needs by OIM should be addressed in the Key Initiative Plan |
| Appendix C | The Interfacing of Internet Claims should be discussed |
| Appendix E, Table E-2 | Included in the risk assessment should be risks from fraud, penetration of systems by hackers, complexity in the use of several DDS systems and the ability to comply with HIPAA. |
| Appendix C, page 2 | If the goal is to only input key data fields once, can we still accept scanning/imaging of handwritten information on the 3368 (self-help) form? Also, how can scanned/imaged data be modified? |
| Appendix C, page 2 | Does the estimate for savings include the conversion of pre-Electronic Folders to electronic formats? What is the plan for converting existing paper folders to electronic versions? |
| Appendix C | Since this document was created in February 2001, some of the items that are shown as future events should have already occurred. Should notes be inserted to provide more current information? For example, on page 6, has OWA finished its review of the impact eDib has on the Delaware processing times? On page 15, how many AS-400 conversions have occurred? On page 23, when will SSA convert to Office 2000 (it did not occur by the end of FY 2000)? |
| Appendix C, page 37 | Could the assumptions and underlying calculations supporting the cost-benefit summary be added or in a footnote, give an intranet site where this information could be found? |

June 14, 2002

NOTE TO NANCY WEBB:

Thank you for the opportunity to comment on the Social Security Administration's (SSA) Accelerated eDib (AeDib) Cost-Benefit Analysis (CBA). The Office of the Inspector General only reviewed the CBA for its overall content, and did not conduct an audit of the document. We therefore, do not express a formal opinion on the CBA at this time.

The CBA prepared by Booz Allen Hamilton, is comprehensive and provides a foundation for moving forward in additional planning and analysis. We have the following comments regarding the SSA AeDib version 2.0a CBA.

## Office of the Inspector General
## Comments on the Booz, Allen & Hamilton eDib Cost Benefit Analysis

| SLIDE | COMMENT |
|---|---|
| overall the scanning contract | The cost of scanning evidence and the accompanying requirements in the contract regarding internal controls in place to ensure the reliability of scanned data should provide assurance to convince a court that the scanned evidence is reliable. In addition, the following are important considerations when dealing with contractors working with electronic services.<br>• SSA needs to set up a protocol, and ensure consistent application across the board. If a trial occurred, the Agency might need an expert who could testify as to how the process works and why it is reliable.<br>• Once the contractor captures the record, there should be controls in place to limit its alterability.<br>• There should be a record of the person capturing the form, which also shows how the record was received and on which date. There should be an audit trail for any later changes to the document.<br>• The medium on which the contractor retains the form should be secure and easily accessible to SSA. The contractor should back-up the information.<br>• The contractor should fully understand legal privacy protections afforded this information. The contract should specify responsibilities, liabilities and recourse.<br>• The contractor should capture the documents in their entirety.<br>• Paper copies should be retained whenever there is suspected fraud. |
| Overall | It is not clear where you obtained and how you verified the projects planning, acquisition, operations and maintenance costs. |
| Page 5 | The security costs should be based on a comprehensive risk analysis. |
| Page 16 | It is not clear where you obtained and how you verified the costs and processing times to perform this analysis of processing time. |

| SLIDE | COMMENT |
|---|---|
| Page 19 | Version 2.0 of the implementation plan calls for full implementation in FY 2007, while 100 percent of the benefits begin in the third year and beyond. Also, doesn't full implementation in FY 2007 conflict with the Commissioner's direction of full completion by December 2003? |
| Page 28 | We are concerned because Booz Allen Hamilton have not yet verified the EDCS costs, yet these costs and the corresponding projected savings are a major factor in the Accelerated eDib project. |
| Page 50 | We have concerns that SSA will not meet its scheduled implementation dates for the IBM AS400 computers. The consequences of not meeting this schedule should be addressed. |
| Page 86 | The costs to store the backup of electronic data seem to be excluded and could be a major undertaking with up to 270 pages of scanned data for each claimant in addition to the initial and postentitlement claims information. |
| Page 105 | Under business to Government, for the benefit of business, we should attempt to accept standard protocols to be used by business under HIPAA. |

If you have any questions about our comments, you may contact me at 410-965-9701, Kitt Winter (965-9702), or Al Darago (965-9710).

Sincerely,

***Steven L. Schaeffer***

ATTACHMENT C

# AeDib Timeline
05/03/02

## Internet Disability

The Internet disability applications collects information currently gathered from the agency's paper disability form. The initial release, I3368 will collect medical and work history from disability claimants. Additional applications will be developed to support the disability process. These applications will collect supplemental disability and more detailed work information, information about childhood disabilities, and information required for subsequent appeal processes. Internet Disability will improve service to the public, compensate for resource losses and workload increases, improve the disability report collection process, and contribute to meeting the Government paper Elimination Act requirements.

| Date | Milestone |
|---|---|
| 8/02 | Production Ready for Initial Functionality of I3368 |
| 1/03 | Production Ready for Internet I827 |
| 4/03 | Production Ready for Fully Functional I3368 |
| 7/03 | Production Ready for Internet I3820 |
| 11/03 | Production Ready for Internet I3369 |
| 12/03 | Production Ready for Internet I3441 |
| 12/03 | Production Ready for Internet I454, I4486, I4631 |

## Electronic Disability Collect System ver 4.2.2

Electronic Disability Collect System (EDCS) provides the means for our employees to collect information about a claimant’s disability. EDCS 4.2.2 is a technical release to convert the EDCS from a client/server application to an intranet application. This release is limited to adult disability cases at the initial adjudicative level.

| Date | Milestone |
|---|---|
| 7/02 | Production Ready (Delaware, Texas, & California) |

## Electronic Disability Collect System ver 4.2.3

Adds the following functionality:

1. Record of Change
2. Subsequent Filings
3. Alternative Methods to Populate the Medical Source Reference File
4. Interface to the Internet 3368

| Date | Milestone |
|---|---|
| 10/02 | Production Ready for Delaware, Texas, & California) |
| 10/02 | Production ready for National Rollout |

## Electronic Disability Collect System ver 5.0

Adds the following types of disability cases

1. Child cases at the Initial adjudicative level
2. Reconsiderations

| Date | Milestone |
|---|---|
| 2/03 | Production Ready |

### Electronic Disability Collect System ver 5.1

Adds the following:

1. Continuing Disability Reviews
2. Continuing Disability Reviews Reconsiderations
3. Hearing Cases
4. All other related forms

| Date | Milestone |
|---|---|
| 5/03 | Production Ready |

### Electronic Disability Collect System ver 6.0

EDCS interface to Electronic Folder using MQSeries as the transport mechanism.

| Date | Milestone |
|---|---|
| 7/03 | Production Ready |

### Electronic Disability Collect System ver 6.1

DDS and SSA Legacy Applications interface to Electronic Folder using MQSeries as the transport mechanism. Includes the storage and retrieval of data to a data repository as well as images and other objects to the Enterprise Document Imaging Architecture (EDIMA).

| Date | Milestone |
|---|---|
| 12/03 | Production Ready |

## Enterprise Document Imaging Architecture

This project will identify and implement the document imaging architecture and infrastructure required to support the AeDIB business process.

| ***Date*** | Milestone |
|---|---|
| 10/02 | Architecture and Infrastructure Recommendations Documented |
| 10/03 | Complete Procurements for EDIMA Infrastructure |
| 1/04 | Complete EDIMA Infrastructure Installation in Required Sites |

## AS400/Legacy Software

This project includes the migration of Wang/Levy states to IBM AS/400 platform; migration of Levy code incorporating readiness for EFI; upgrade/replacement of existing AS/400s in order to accommodate EFI; readiness of Versa, Midas, and independent software systems for EFI.

Group 1 States = VA, WV, MD, WI, IN, GA, AR, OH, OK, IA, NC, FL, NM, RI, SD, FDDS
Group 2 States = KS, MA, WA, DC, KY, MT, CT, MI, CO, AZ, LA, VT, PR

| Date | Milestone |
|---|---|
| 6/02 | Installation of AS/400 Complete for RI, SD, KS, MA, FDDS |
| 9/02 | AS/400 Training Completed for RI, SD, KS, MA, FDDS |
| 9/02 | Installation of AS/400 for DC, KY, MT, CT, MI, CO, AZ, LA, VT, PR |
| 10/02 | VERSA and LEVY Pre-Implementation in support of EDCS 4.2.3 |
| 12/02 | AS/400 Training Completed for DC, KY, MT, CT, MI, CO, AZ, LA, VT, PR |
| 12/02 | Complete Business Process Description for NY, NE, and Midas states. |

### AS400/Legacy Software

| | |
|---|---|
| 12/02 | Production Ready "ALL" - Group 1 States |
| 10/03 | **Production Ready "ALL" - Group 2 States** |

### *The OHA Case Processing and Management System*

The OHA Case Processing and Management System will provide automation to the Hearing Offices activities.

| Date | Milestone |
|---|---|
| 10/02 | Determine Systems Design |
| 12/03 | Pre-Production Implementation |
| 1/04 | Production Ready |

### *Complete Business Process Description*

| Date | Project |
|---|---|
| 6/02 | OHA, Operations, Office of Quality Assurance and Office of Disability |

October 16, 2002

NOTE TO BILL GRAY:

SUBJECT: Office of the Inspector General's (OIG) comments regarding SSA's Project Scope Agreement (PSA) for Enterprise Document and Imaging Management Architecture (EDIMA) for Accelerated Electronic Disability (AeDib) Project

The Social Security Administration's (SSA) OIG has obtained the Agency's PSA for the EDIMA for the AeDib Project. We have discussed the PSA with various Agency staff and evaluated the document's potential effect on SSA's ability to assess the integrity of the data this system will process and contain. Our overall comment is that we could not find the internal control/security risk assessment used as a basis for the EDIMA. Federal requirements and the Agency's Project Development Resource System (PRIDE) call for the internal control and security requirements of major system development projects to be based upon a risk assessment. If the risk assessment is available, it should be attached to the document to provide a point of reference for the security/control assessments. In addition, there are some features that SSA should reconsider before deferring them.

- Currently, the system requirements defer an audit trail that would track user access to internal and external systems. An audit trail is an essential part of any new system and we believe the Agency should reconsider deferring its development, unless compensating controls are utilized.
- The EDIMA also defers the ability to "lock" electronic forms (e.g. Workers compensation offset forms) to prevent further annotation or modification to indexing fields. Lock provisions are an essential part of the internal controls necessary to establish the originator of the transaction and that the transaction has not been altered. These controls help ensure successful fraud prosecution.
- The ability to restrict access to all or portions on a repository structure and to limit subsequent access to read-only is deferred. To secure its data an ability to limit subsequent access is essential. This deferral when combined with the deferral of the audit trail and the locking feature could allow individuals to change data without recording the individual that changed the data.
- The ability to encrypt images and data documents selectively using a standard encryption algorithm is also deferred. Such a control over claimant data would be useful in protecting individual privacy.
- The ability to accept digital signatures and public key infrastructure has also been postponed. The Agency should begin moving forward in this area, since Federal law encourages the use of electronic signatures.
- The document does require business continuity but does not specify what documents will be backed up off-site.
- The document does not call for a structured approach to data. The Agency should attempt to structure as much data as possible. Structured data would allow the

Agency to accumulate and gather the data for management information and future processing purposes.

- The document does not discuss any management information requirements of the system.

Finally, the document appears to be developed and controlled primarily by SSA's Office of Systems. If this is the case, we believe system development projects should instead be user driven, because the user is most familiar with any needs that they will have when the system is operational.

If you should have any questions regarding our comments, please give me a call at extension 59700 or have your staff contact Al Darago on extension 59710.

Gale S. Stone