U.S. DEPARTMENT OF LABOR

Office of Inspector General

EFAST General Controls Need Strengthening

U.S. Department of Labor
Office of Inspector General
Report No. 09-01-001-12-001

Date:

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION 3

OBJECTIVE, SCOPE, AND METHODOLOGY 5

FINDINGS AND RECOMMENDATIONS 7

1. The EFAST Risk Assessment Implementation and Testing Need Improvement 8

2. The EFAST Continuity of Operations Plan Needs to be Improved and Tested 13

3. NCS Management Needs to Strengthen Information Security Officer Position 18

APPENDIX A 22

PWBA Comments on Draft Report

ACRONYMS

COOP	Continuity of Operations Plan
DOL	Department of Labor
ECP	Engineering Change Proposal
EFAST	ERISA Filing Acceptance System
ERISA	Employee Retirement Income Security Act of 1974
FISCAM	Federal Information System Controls Audit Manual
GAO	General Accounting Office
IRS	Internal Revenue Service
ISO	Information Security Officer
NCS	National Computer Systems, Inc.
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PBGC	Pension Benefit Guaranty Corporation
PWBA	Pension and Welfare Benefits Administration

EXECUTIVE SUMMARY

The Office of Inspector General conducted an audit of the general controls over the Pension and Welfare Benefits Administration's (PWBA) Electronic Filing Acceptance System (EFAST). Our primary objective was to determine if the EFAST has adequate and effective general controls to protect filings and prevent unauthorized disclosure or modification of sensitive data, or disruption or denial of critical services.

Overall, we concluded that PWBA management has devoted substantial resources and made significant progress in developing the necessary security plans, performing risk assessments and security reviews, and coordinating complex security requirements between the Internal Revenue Service (IRS) and its contractor, National Computer Systems, Inc.(NCS). However, PWBA management needs to take additional action to improve the security of the EFAST. Specifically, PWBA management needs to ensure that NCS management (1) improves the EFAST's Risk Assessment implementation and testing, (2) fully develops and implements the Continuity of Operations Plan (COOP), and (3) strengthens the Information Security Officer (ISO) position.

The EFAST Risk Assessment Implementation and Testing Need Improvement

PWBA management needs to improve the EFAST's Risk Assessment implementation and testing. Specifically, (1) the EFAST Risk Assessment does not cover unprocessed filings, (2) many of the controls planned were not implemented, and (3) some of those implemented were never tested. As a result, the EFAST is operating at a risk level that is above the maximum acceptable level established by PWBA.

The EFAST COOP Needs to be Improved and Tested

PWBA management needs to require NCS to more fully develop and implement the EFAST COOP. This occurred because PWBA and NCS management have devoted most of their resources to getting the system operational and have not focused on the COOP. As a result, while the EFAST is operational, it is highly vulnerable to disruptions, disasters, and loss of original unprocessed Form 5500 Series filings.

NCS Management Needs to Strengthen ISO Position

NCS management needs to strengthen its ISO position. NCS management has not provided the necessary job description, training, or written procedures to the ISO. NCS management has devoted its attention to implementing the EFAST and only recently hired an onsite ISO. As a result, the ISO is not aware of security problems and is not adequately involved in security issues.

In conducting our audit, we used the General Accounting Office's (GAO) Federal Information System Controls Audit Manual (FISCAM). We conducted interviews and tests both at PWBA headquarters and its contractor locations in Kansas and Virginia. Our audit was performed between September 12, 2000, and January 10, 2001, and was conducted in accordance with *Government Auditing Standards*.

We recommend that the Assistant Secretary for Pension and Welfare Benefits improve and test the EFAST Risk Assessment, fully implement the COOP, and ensure that NCS improves its ISO position.

Summary of PWBA Response

In response to the draft report, PWBA generally concurred with the findings and recommendations. PWBA had already requested and received an engineering change proposal (ECP) from NCS that addressed many of the OIG's findings and recommendations. PWBA pointed out, however, that there is an administrative process which must be followed to make these changes. Any contract modifications would have to be negotiated by the Department's procurement staff, and the time frames for these actions were not within PWBA's control.

PWBA additionally stated that the agency had already taken significant action towards correcting the shortcomings detected by the OIG audit and has had regular discussions with NCS on these issues. For example, PWBA conducted a security retest of the EFAST facility that addressed many of the OIG's findings and recommendations regarding security controls that were either not tested or never implemented. PWBA also stated it was on track to overhaul and test the Continuity of Operations Plan (COOP) in response to the OIG's finding that the COOP was not fully developed, implemented, or tested.

PWBA's response to the draft report in its entirety is attached to this report as Appendix A.

INTRODUCTION

Background

The Employee Retirement Income Security Act of 1974 (ERISA), and provisions of the Internal Revenue Code, assigned responsibility for regulating employee benefit plans to three Federal agencies: the Department of Labor (DOL); the IRS; and the Pension Benefit Guaranty Corporation (PBGC). Within the DOL, PWBA has responsibility for oversight of employee benefit plans.

To meet their oversight responsibilities, all three agencies use information provided by employee benefit plans in their annual reports. These annual reports use the Form 5500 Series for providing the necessary information. Until 2000, plans filed the annual reports with the IRS. In August 2000, PWBA set up a new processing system for the Form 5500 Series called the EFAST.

The purpose of the EFAST is to process the paper and electronic Form 5500 Series filings into computer-readable format and provide PWBA, IRS, PBGC, and the Social Security Administration with comprehensive, accurate, and timely data.

To meet this purpose, in 1997 DOL issued a Request for Proposals for the development and operation of the EFAST to replace the IRS process. In September 1998, DOL awarded a contract to NCS to develop the EFAST system. In August 2000, the EFAST started processing Form 5500 Series filings.

The primary EFAST facility, shown on the right, is located in Lawrence, Kansas. Software development by a subcontractor is being done in Reston, Virginia.

PWBA management expects the EFAST to handle approximately 1.5 million Form 5500 Series returns filed annually by plan administrators and sponsors. Plan administrators file most of these returns on paper, although PWBA management expects the percentage of filings filed electronically to grow.

Principal Criteria

The principal criteria we used in our audit included:

- OMB Circular A-130: Management of Federal Information Resources.
- NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook.
- NIST Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems.
- NIST Special Publication 800-18: Guideline for Developing Security Plans for Information Technology Systems.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

Our audit objective was to determine if the EFAST has adequate and effective general controls. These general controls include management, operational, and technical computer security controls in place to prevent unauthorized disclosure or modification of sensitive data, or disruption or denial of critical services.

Scope

We designed this audit to assess the effectiveness of general controls in the EFAST. We identified, evaluated, and tested the general controls required to protect sensitive data from the many threats that exist. These threats include, but are not limited to, fraud and abuse, data entry errors, cyber-attacks, natural disasters, utility disruptions, and espionage.

Specifically, we evaluated controls intended to:

- protect data, files, and programs from unauthorized access;
- prevent unauthorized changes to systems and applications software;
- provide segregation of duties between applications and systems programmers, computer operators, security administrators, and other data center personnel;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure adequate computer security administration.

We performed our work according to *Government Auditing Standards* issued by the Comptroller General of the United States. Our audit included such tests of policies and procedures and other auditing procedures we considered necessary in the circumstances.

Methodology

This audit applied the methodology outlined and described in GAO's FISCAM. This manual provides guidance and recommendations to test general controls in both General Support Systems and Major Application Systems.

During the audit, we visited PWBA's headquarters and the NCS operated EFAST facility in Lawrence, Kansas. We also visited Logicon, the software developer, offices in Reston, Virginia. We interviewed PWBA EFAST officials as well as NCS and Logicon personnel.

To evaluate the controls, we identified and reviewed PWBA's and NSC's general control policies and procedures. Through this review and discussions with PWBA and NSC staff, including programming, operations, and security personnel, we learned how the general controls were designed to work and the extent data center personnel considered them in place. We also reviewed PWBA's and NSC's systems and security software installation and use.

Further, we tested and observed the operation of general controls over the EFAST to determine whether they were in place, adequately designed, and operating effectively. Our tests included attempts to obtain access to sensitive data and programs, which we performed with the knowledge and cooperation of PWBA and NSC officials.

We held an entrance conference on September 12, 2000, and completed our fieldwork on January 10, 2001. We held an exit conference with PWBA headquarters on February 14, 2001. At that meeting, we discussed our findings and recommendations.

FINDINGS AND RECOMMENDATIONS

PWBA and NCS management have devoted large amounts of resources to the EFAST security and have given overall system security a high priority in system development. However, additional actions are needed to ensure that the EFAST security meets minimum requirements for reducing risk to an acceptable level for operations. Specifically, PWBA management needs to ensure the EFAST Risk Assessment is fully implemented and tested, the COOP is more fully developed and tested, and that NCS management strengthen its ISO position to reduce the EFAST's vulnerability.

1. The EFAST Risk Assessment Implementation and Testing Need Improvement

PWBA management needs to improve the EFAST's Risk Assessment implementation and testing. Specifically, (1) the EFAST Risk Assessment does not cover unprocessed filings, (2) many of the controls planned were never implemented, and (3) some of those implemented were never tested. PWBA management oversight emphasized getting the system operational and did not ensure NCS management fully complied with the EFAST Risk Assessment. Also, the EFAST Security Plan NCS officials developed set the sensitivity level too low which contributed to the problem. As a result, the EFAST is operating at a risk level that exceeds the maximum risk acceptable under the PWBA contract.

Risk Assessment Requirements

OMB Circular A-130 establishes that certain Federal information systems require special attention to security due to the importance of the system to an agency's mission. The Circular defines these systems as "major applications" and requires that these systems be considered "high risk" due to their importance. This "high risk" assignment then provides the basis for a security plan and risk assessment. PWBA management has designated the EFAST a "major application."

The risk assessments the Circular requires Federal agencies to develop are to identify threats, vulnerabilities, and the effectiveness of current or proposed safeguards. The Circular further requires these safeguards to be tested to determine if they are operational.

The contract PWBA awarded to NCS required NCS management to develop a security plan and a risk assessment and to test the controls.

EFAST Risk Assessment Needs Improvement

PWBA management emphasized getting the system operational and did not ensure NCS management fully implemented the controls identified in the EFAST Risk Assessment or tested the controls to confirm they were operational.

Contributing to both the development and testing issues of the EFAST Risk Assessment was that the EFAST Security Plan identified the EFAST as a major application but only assigned a "medium" level of risk to the system. This contradicts OMB Circular A-130 which requires major applications such as the EFAST to be considered "high risk."

Security Controls Not Implemented - The EFAST requires confidentiality because it processes sensitive tax data. It also requires integrity and reliability because of the reliance PWBA, PBGC, and the IRS place on the system for providing information critical to each agency's mission. The EFAST Risk Assessment completed by NCS identified 261 separate controls which were to be built into the EFAST to minimize risk and help ensure confidentiality, integrity, and reliability.

However, PWBA management did not ensure NCS management implemented all controls identified. These controls are among those selected in the EFAST Risk Assessment as a minimum level of control necessary to provide an acceptable level of risk to the EFAST. Since some of these controls have not been implemented, the EFAST is operating below the minimum level of control PWBA management determined to be acceptable.

Examples of controls not implemented follow:

- The EFAST Risk Assessment included installing a water drain as a protection against water damage. However, PWBA management did not ensure NCS personnel installed a water drain or other water protection, in either the computer room or the warehouse where the unprocessed Form 5500 Series filings are kept. Both areas contain a sprinkler system which could develop leaks and allow water into the areas causing damage. As shown in the picture to the right, the warehouse is used to store over a million unprocessed Form 5500 Series filings. These paper filings are easily subject to water damage if the presence of water is not detected.

- The EFAST Risk Assessment states that any media to be reused will be

degaussed or overwritten. This procedure would protect the confidentiality and integrity of data.

- The EFAST Risk Assessment states that a management control will be established to ensure that all changes to the EFAST hardware or software that could in any way lessen security will be reviewed and approved by the ISO. This control would help ensure security continuity.

- The EFAST Risk Assessment states that all changes to the EFAST software will be reviewed and approved by management. However, the EFAST Program Manager, who has approval authority, is not documenting this approval on the required forms.

Controls Not Tested - In addition to some controls not being implemented, we found that NCS officials did not test many controls identified in the EFAST Risk Assessment. While the EFAST Risk Assessment identified 261 separate controls that NCS officials would use in the EFAST, NCS officials actually tested 222. The remaining 39 controls were not tested. The EFAST Risk Assessment included these 39 controls as comprising the minimum acceptable level of control.

Examples of controls not tested include:

- Procedures to ensure NCS management maintains accountability records for keys to the EFAST area doors.

- Procedures to ensure NCS management maintains remote terminal identifiers for remote terminals used to access the EFAST in a protected file.

- Procedures that require remote terminals used to access sensitive information be protected with physical and technical security controls. At any one time, EFAST has more than 50 programmers, including subcontractors, with remote access to the system from outside locations.

Overall, NCS management did not test a significant amount (39 of 261) of the controls identified as the minimum acceptable level of control in the EFAST Risk Assessment and neither PWBA nor NCS management has any assurances that these controls exist and are functioning.

Conclusion

PWBA management did not ensure NCS fully implemented and tested the controls the EFAST Risk Assessment identified as the minimum necessary as acceptable for the EFAST.

PWBA management did, however, authorize the EFAST to start processing. Authorization implies PWBA management is accepting the risk in the entire application, although to this date, the EFAST Risk Assessment is incomplete and cannot ensure that the EFAST is achieving an acceptable level of risk for processing Form 5500 Series sensitive data. This condition exposes sensitive confidential tax information to unauthorized disclosure, possible litigation risks, and loss.

Recommendations

We recommend the Acting Assistant Secretary for Pension and Welfare Benefits:

a. Revise the Security Plan to reflect higher risk and determine if any changes are necessary to the EFAST Risk Assessment to reflect the higher risk recognized.

b. Require NCS management to implement and test each control included as a minimum for acceptable processing.

PWBA's Comments on Draft Report

In its response to the draft report PWBA stated:

> PWBA generally concurs with the OIG's findings and recommendations regarding the EFAST security plan and risk assessment. PWBA plans to address these shortcomings through a combination of efforts including: revising the security plan and developing a risk mitigation plan to verify the applicability of all security controls, fully implementing the applicable security controls, and ensuring that all security controls established for EFAST are adequately tested.

PWBA concurred with each recommendation and stated:

PWBA is scheduled to update the Computer Security Plan by late June 2001 which will designate EFAST as a high risk application. PWBA does not believe that any changes are necessary to the EFAST Risk Assessment to reflect the higher risk recognized because the EFAST Risk Assessment incorporated the C2 level security requirements which were determined to be appropriate. However, as stated above, PWBA will develop a Risk Mitigation Plan to address the OIG's overriding concern that risk mitigation measures be instituted to address security controls that have not been tested or implemented.

PWBA also pointed out some wording in the draft report which could be confusing or misleading.

OIG Evaluation of PWBA Comments

We made changes to the wording in the draft report as PWBA suggested.

PWBA responses are sufficient to resolve the recommendations. The recommendations will be closed when the corrective actions are complete.

2. The EFAST COOP Needs to be Improved and Tested

PWBA management has not ensured NCS management fully developed or implemented the EFAST COOP. This is because PWBA and NCS management have devoted most of their resources to getting the EFAST operational. As a result, while the EFAST is operational, it is operating with high vulnerability to disruptions, disasters, and loss of original unprocessed Form 5500 Series filings.

COOP Requirements

OMB Circular A-130 specifically requires each government entity's major application to have a COOP. The Circular states that a COOP should include system backup policy and procedures and one or more recovery strategies to cover partial loss of equipment or service due to disasters.

Also, OMB Circular A-130 and NIST Special Publication 800-14 require testing of the COOP. Specifically, NIST Publication 800-14 Section 3.6.5 states that an organization needs to test its COOP because there will undoubtedly be flaws in the COOP.

As required by the contract with PWBA, NCS management prepared a COOP which PWBA management accepted on June 15, 2000. The COOP calls for recovery of any disruption within 30 days. It analyzes the risks of operational disruption and describes the controls and actions necessary to reduce such disruption.

COOP Needs Improvement

PWBA management, however, has not ensured that NCS management (1) developed the COOP to cover unprocessed filings, or (2) implemented all the controls and support actions described in the COOP. Several vulnerabilities exist that could affect the EFAST processing and delay restoring service in case of disaster. The following sections discuss several vulnerabilities.

Water Danger to Filings Not Covered - The EFAST COOP deals with two potential water problems--natural flood and water supply leaks. The initial response and action procedures cover protecting the computer equipment. These procedures do not cover protecting the unprocessed filings. The filings are stored next to the EAST processing area. Water

sprinklers and pipes are directly above the uncovered filing storage bins as shown in the photograph on page 9.

NCS officials do have protective plastic sheets to cover the filings to protect them from water damage. However, the plastic sheets were locked in a file cabinet. The sheets consisted of four small rolls of clear plastic that appeared to cover approximately 200 square feet. These rolls would not cover even a small fraction of the filings.

Data Backups Not Performed - The COOP requires that the EFAST databases be backed up daily. This, however, is not being done. According to the daily backup log, NCS officials did not do any backups from the time the EFAST processing started on July 1, 2000, until October 18, 2000. During this time, NCS management processed more than 164,000 filings and schedules without any backup. Additionally, according to the backup log, NCS officials did not perform backups on 13 of the 29 work days from October 18, 2000, through November 27, 2000.

Emergency Procedures Do Not Cover Filings - Neither the COOP nor NCS' emergency procedure manual includes procedures for protecting or recovering actual Form 5500 Series filings. The emergency procedures in both documents include detailed steps to follow in evacuating the building in case of fire, tornado, or evacuation drill. The documents also cover steps to take to protect the system hardware and software. However, the documents do not have procedures to guide personnel to protect the paper filings that await processing in case of a water leak or any other emergency. If an emergency or disaster were to occur, the actual paper Form 5500 Series filings may be subject to loss or destruction.

Alternate Processing Site Not Implemented - The COOP, as required, specifies an alternate processing site in the event a disaster damages the EFAST facility. The COOP specifies a particular company to provide back-up facilities and details on how that company will make facilities available. However, NCS management has not executed a contract with this company or even confirmed that the company is still available for back-up protection. As a result, NCS management does not have assurances that, if the EFAST facility became inoperable, there would be any back-up facility at all or when one could be provided.

COOP Not Tested as Required - The EFAST COOP states that NCS will test the COOP. However, NCS management did not test the COOP as part of the overall system testing and NCS management does not plan to perform testing at all. EFAST has been operating since

July 1, 2000. We believe that the COOP should have been tested as part of the overall system testing. As a minimum, NCS management should have plans as to when and how testing will be performed. Without testing, NCS management does not have assurances that their planned recovery procedures will be effective.

Conclusion

We concluded that the COOP needs to be improved and tested to be effective. This is necessary to ensure that NCS personnel can quickly and appropriately respond to emergencies and that the EFAST and its data will be adequately protected. This is particularly true for two reasons. First, the EFAST provides necessary information for three different agencies; PWBA, IRS and PBGC. It also provides some information to the Social Security Administration. Therefore, although PWBA operates the EFAST, it must be responsive to the needs of the other agencies. Secondly, in the near future the EFAST will be providing on-line capability to PWBA, PBGC and IRS with over 300 direct users planned. As on-line usage increases, the reliability of the system becomes more critical. Therefore, PWBA management needs to take action to improve the EFAST contingency planning.

Recommendations

We recommend that the Acting Assistant Secretary for Pension and Welfare Benefits require NCS management to:

a. Revise the COOP to specifically provide for damage to the paper Form 5500 Series filings.

b. Implement all procedures and controls identified in the COOP, including but not limited to, alternate site selection and data backup.

c. Test the COOP and determine its effectiveness.

PWBA's Comments on Draft Report

PWBA concurred with this finding and stated:

PWBA concurs with the OIG's findings that the COOP has not been fully developed, implemented, or tested. PWBA plans to address these shortcomings by updating the COOP, following through to ensure that all COOP controls are implemented, and fully testing the COOP.

As a point of clarification, PWBA would like to point out an inconsistency in the wording in the draft audit report which might be confusing or misleading regarding the COOP. The Executive Summary states on page 1 that "the EFAST COOP needs to be developed and implemented." PWBA believes this statement is somewhat misleading because it implies that a COOP was not developed and implemented, when it was. However, in the summary of Findings and Recommendations, the report specifies on page 12, 1st bullet, that "PWBA management has not ensured NCS management fully developed or implemented the COOP."

Regarding the specific recommendations, PWBA concurred and stated:

PWBA has requested and received an ECP from NCS which covers, among other things, the upgrading of the EFAST facility to protect against sprinkler mishap. We are acutely aware of the need to protect unprocessed paper filings from water damage arising from sprinkler mishap. To address this potential hazard, the ECP contains several important enhancements to the water sprinkler system. Specifically, NCS proposes to upgrade the sprinkler system to a pre-action valve, wet system in the EFAST production area and warehouse to better protect the EFAST 5500 forms. In the interim period prior to implementing the provisions of the ECP, NCS has secured and put in place sufficient plastic sheeting to cover the filings to protect them from water damage.

. . . . NCS is scheduled to update and deliver a new version of the COOP to PWBA by late June 2001. This is a regularly scheduled update to the COOP that is called for in the EFAST contract. PWBA intends to notify NCS of all remaining COOP shortcomings identified by the OIG and will insist that all deficiencies are remedied in the new version of the COOP, and that the procedures and controls are in place, such as alternate site selection and data backup. This action will specifically address the OIG's findings concerning: 1) data backups not performed, 2) emergency procedures do not cover filings, and 3) alternate processing site not implemented.

. . . . PWBA intends to strictly enforce all contractual provisions regarding the COOP, such as the requirement to test the COOP per OMB Circular A-130 and NIST Special Publication 800-14. Upon delivery of the final COOP in late June 2001, PWBA will follow-up with NCS to ensure that all procedures and controls identified in the COOP are implemented.

OIG Evaluation of PWBA Comments

PWBA's concurrence is sufficient to resolve the recommendations and they will be closed when the COOP is updated, implemented and tested. In addition, we have made changes to the final report to clarify that PWBA had required that a COOP be developed.

3. NCS Management Needs to Strengthen ISO Position

NCS management needs to strengthen its ISO position. NCS officials have not provided the necessary job description or training to the ISO. Nor does NCS have written security procedures.

OMB Circular A-130, Appendix III states that sound and effective information security management requires that a management official be assigned responsibility for security of the data and system. This management official needs to be knowledgeable (1) about the information and process supported by the application and (2) in the management, personnel, operational, and technical controls used to protect it. The Circular states that this official shall ensure that effective security products and techniques are appropriately used in the application. This official is to be contacted when a security incident occurs.

Moreover, NIST Special Publication 800-14 Section 2.5 states that the responsibilities and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit.

ISO Position Needs Strengthening

NCS management has designated the ISO position to be responsible for the EFAST security. However, the ISO does not have the necessary management tools to accomplish the ISO duties most effectively. Specifically, NCS management has not developed a job description to establish ISO responsibilities clearly, provided sufficient ISO training, or written security review procedures.

No Job Description - NCS management has not developed a job description for the EFAST ISO. This is a basic management tool needed to ensure that the ISO, the ISO's supervisors and other NCS and PWBA personnel understand the ISO mission, functions, and responsibilities. An ISO job description would be an integral part of explicitly defining the ISO responsibilities.

Also, without a job description, NCS management has not provided the ISO sufficient authority to accomplish the ISO duties and responsibilities. While the ISO is charged with maintaining the EFAST integrity and security, the ISO has only limited access to the EFAST and cannot directly monitor computer security activity. For example, the ISO does

not have a computer terminal that accesses the EFAST. The ISO must use another employee's terminal to do this. Also, the ISO does not have sufficient system authority to review the on-line EFAST security log. This log is readily accessible to other EFAST employees. The ISO relies on obtaining a printed copy of the EFAST security log each week from the system administrator.

Training is Needed - NCS management has not provided sufficient training to the ISO position. We reviewed the ISO's personnel file and found that the only training NCS management provided was a one-week security training course. While the current ISO is highly qualified in IT systems technology, job specific training is necessary to ensure that the ISO effectively manages security.

No Written Security Procedures - NCS does not have written security procedures. Such procedures are needed for the ISO to follow or to inform NCS management how the security program will function. NCS management does not have any specific procedures for determining the frequency of security reviews or how the ISO will perform the reviews. Other than day-to-day contact with the ISO, NCS management has no method to determine how the ISO position will function in the EFAST environment.

These weaknesses in security management have allowed specific security problems to occur, as discussed below.

- During our visit to the EFAST facility, we could enter the EFAST restricted area without badges or authorization through an unlocked back door. Subsequently, NCS officials discovered two other unlocked doors that were supposed to be locked. All three doors had faulty locks. NCS management had not clearly identified the responsibility for ensuring these doors were locked.

- The electronic filing firewall was disabled without the ISO's knowledge. The EFAST accepted more than 15,000 filings without benefit of a working firewall. When NCS brought the EFAST online, the system would not work with its existing firewall. NCS and PWBA officials decided to disable the firewall and accept the electronic filings without the protection. They made this decision without the involvement of or input from the ISO who is responsible for overall EFAST security.

- The ISO reviews the EFAST computer security log weekly, not daily as required by NIST Special Publication 800-14. The EFAST ISO, however, does not have

sufficient system access to do this. In fact, as previously noted, the ISO does not have a direct access to the system online. Instead, the ISO relies on the system administrator to furnish a printed log each week.

Conclusion

NCS management needs to improve security management to prevent these types of incidents from occurring. Effective security management requires developing an ISO job description, providing additional ISO security training, and developing written security procedures.

Recommendations

We recommend that the Acting Assistant Secretary for Pension and Welfare Benefits require NCS management to:

a. Develop a comprehensive written job description for the ISO, including delegating appropriate authority.

b. Provide additional security training to the ISO.

c. Develop written procedures that detail the ISO's procedures to ensure that NCS management (1) maintains proper EFAST security, including physical security, and (2) consults or informs the ISO regarding all EFAST security changes.

PWBA's Comments on Draft Report

PWBA concurred with this finding and stated :

> PWBA concurs with the OIG's findings and recommendations regarding strengthening the ISO position. PWBA plans to address these shortcomings through the ECP described above, which, among other things, will bolster the position and update and maintain the "EFAST Security Procedures Manual."

PWBA clarified that it had required written security procedures for EAST. PWBA stated:

> A point of clarification is necessary regarding the OIG's finding that "NCS does not have written security procedures." As a condition of the EFAST security certification process, PWBA directed that NCS develop written security procedures that describe the duties and responsibilities of the ISO. NCS subsequently developed a document entitled "EFAST Security Procedures Manual" that describes the NCS security procedures. A draft, "working" version of this document was delivered to PWBA by NCS in February 2001--and it addresses the majority of the OIG's concerns regarding the lack of written security procedures. The document will continue to be updated and maintained through the life of contract.

On the recommendations, PWBA stated the security-related ECP solicited from NCS included strengthening the ISO position. The security ECP also covered the provision of additional security training to the ISO. PWBA also stated that it would require NCS to continue to develop, update, and maintain security procedures to ensure that NCS management (1) maintains proper security, including physical security, and (2) consults or informs the ISO regarding all security changes.

PWBA anticipated these actions would be completed by the end of FY 2001.

OIG Evaluation of PWBA Comments

At the time we completed out fieldwork in January 2001, NCS had not yet developed the EFAST written security procedures.

However, we believe that these procedures, when finalized, in conjunction with other PWBA corrective actions, are sufficient to resolve the recommendations. The recommendations will be closed when the security procedures are finalized and approved and the ECP process PWBA described is completed.

APPENDIX A

PWBA Comments on the Draft Report