

Office of Inspector General

**U.S. Department of Labor
Office of Information Technology Audits**

Security Testing and Evaluation Pilot Audit of the New Automated Support Package (ASP) Black Lung System

**Report Number: 17-01-003-04-433
Date Issued: March 29, 2002**

TABLE OF CONTENTS

ACRONYMS	i
EXECUTIVE SUMMARY	1
INTRODUCTION AND BACKGROUND	4
CHAPTER I – POSITIVE SECURITY CONTROL AUDIT OBSERVATIONS	6
CHAPTER II – FINDINGS AND RECOMMENDATIONS	8
Finding 1: High-Risk Management Security Control Issues	8
Finding 2: Medium-Risk Management and Technical Security Control Issues	14
OBJECTIVES, SCOPE AND METHODOLOGY	A - 1
GLOSSARY	B - 1
MANAGEMENT RESPONSE TO DRAFT REPORT	C - 1

ACRONYMS

ASP	Automated Support Package
BIND	Berkley Internet Name Domain
BDC	Backup Domain Controller
CSC	Computer Science Corporation
CSPP	Cyber Security Program Plan
DCMWC	Division of Coal Mine Workers' Compensation
DITMS	Division of Information Technology Management Service
DOL	Department of Labor
ECN	Enterprise Computing Network
ESA	Employment Standards Administration
FBLP	Federal Black Lung Program
FIPS	Federal Information Processing Standards
HTTP	HyperText Transport Protocol
IIS	Internet Information Server
IP	Internet Protocol
ISS	Internet Security Scanner
LAN	Local Area Network
MBO	Medical Benefit Only
NCP	NetWare Core Protocol
NetBIOS	Network Basic Input Output System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer

OIG	Office of Inspector General
OMB	Office of Management and Budget
PDC	Primary Domain Controller
PDD-63	Presidential Decision Directive – 63
PMP	Project Management Plan
RDS	Remote Database Services
SAM	Security Accounts Manager
SMB	Server Message Block
SMTP	Simple Mail Transport Protocol
SSP	System Security Plan
ST&E	Security Test and Evaluation
TCP/IP	Transport Control Protocol/Internet Protocol
WAN	Wide Area Network

EXECUTIVE SUMMARY

The Division of Coal Mine Workers' Compensation (DCMWC)/Federal Black Lung Program (FBLP) is currently in the process of implementing a new client-server based system to support the mission of the FBLP. The New Automated Support Package (ASP) Black Lung System will replace the current system, which currently resides on a mainframe computer. The New ASP application and its supporting network infrastructure have been identified by the U.S. Department of Labor (DOL) as a Presidential Decision Directive – 63 (PDD-63) system.

The Office of Inspector General (OIG) has performed a Security Testing and Evaluation (ST&E) pilot audit on the New ASP - Black Lung System. The objectives of the ST&E audit were to determine whether the management and technical security controls over the New ASP Black Lung System and its supporting network environment will sufficiently protect the Black Lung data.

The management and technical security control practices of the FBLP and specifically the New ASP Black Lung System, were compared to guidance from the Office of Management and Budget (OMB) Circular A-130 Appendix III, National Institute of Standards and Technology (NIST) 800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems, and the Critical Infrastructure Assurance Office (CIAO) – Vulnerability Assessment Framework. The ST&E audit was performed in accordance with the United States General Accounting Office's - *Government Auditing Standards* (GAS), issued by the Comptroller General of the United States.

The security issues identified during the audit are divided into three main sections:

- Positive Security Observations
- High-Risk Management Security Control Issues
- Medium-Risk Management and Technical Security Control Issues

Positive Security Control Observations

During the course of the audit, there were a number of positive security control observations identified. Our external scans of FBLP's Internet accessible network devices did not identify potential vulnerabilities on the FBLP's network. There were no vulnerabilities identified for the DOL Employment Standards Administration (ESA) firewall or devices that can be used to connect to the FBLP network, via Internet access. During our internal vulnerability assessment, the audit team was successfully prevented from securing access to the FBLP's two Sequent SE30 Informix database servers. The New ASP client server version of the Black Lung databases will reside on these servers. Additional positive security control observations are contained on page 10 of the report.

High-Risk Management Security Control Issues

During the audit, there were six high-risk management security control issues identified. These include:

- 1) The FBLP – New ASP Black Lung System Security Plan (SSP) has not been finalized.
- 2) A contingency plan has not been completed for the New ASP Black Lung System.
- 3) New ASP Black Lung System client-server security procedures for monitoring and auditing of system activities have not been formally documented.
- 4) Standards are not fully documented for determining access rights to security screens within the New ASP Black Lung System.
- 5) Procedures have not been established for reviewing the New ASP audit documentation: Security Transaction Audit Table and Security Transaction Audit Report.
- 6) Procedures have not been finalized to monitor/audit the UNIX environment on a periodic basis once the New ASP application goes into production.

These six management security issues are high-risk because they would have the potential effect of increasing the risks of unnecessary system downtime, misuse and destruction/exposure of critical Black Lung data. To emphasize, the SSP and contingency plan need to be completed and approvals obtained from the system owner and the Chief Information Officer prior to implementation, as these provide a foundation for implementing and maintaining any system securely. However, the SSP and the contingency plan will not be implemented prior to the April 9, 2001 roll-out date of the New ASP Black Lung System.

Medium-Risk Management and Technical Security Control Issues

There were 25 medium-risk management security control issues identified, which are related to the New ASP Black Lung System, FBLP's current operating environment, and the DCMWC district office sites. These 25 medium-risk security control issues are important in that they also protect the integrity, availability, and confidentiality of Black Lung data.

Management Response

The audit team communicated to DCMWC, the preliminary management and technical security control issues on December 11, 2000. DCMWC management concurred with many of the identified security control issues. Further, DCMWC provided written

responses to many of the management and technical security issues, which included a plan of action to resolve many of the issues in conjunction with the New ASP Black Lung System implementation. In addition, the audit team observed that the FBLP staff has corrected some of the identified security issues.

In management's March 27, 2001 response to the draft audit report, management strongly disagreed with the OIG conclusion reached for the high-risk management security control issues identified during the audit. Management stated that DCMWC has already addressed each of the identified issues. Further, given the inherent strengths of the New ASP Black Lung System, it is highly unlikely that the potential effects stated in the report would occur. For the 25 medium-risk management and technical security control issues identified in the report, management stated that DCMWC has addressed all but two of the issues – password protected screen savers and dry-pipe fire suppression for the District Offices. Management will evaluate the feasibility of resolving these issues in the future.

It should be noted that not all of the DCMWC's responses and actions were verified by the audit team because the management responses were provided after the completion of fieldwork.

Conclusion

DCMWC disagreed with respect to the six high-risk issues for the purpose of delaying system roll out. Instead, DCMWC indicated actions were being taken to address each of these issues but that in doing so most issues may not be resolved until after system rollout. Given this application and general support system is identified as a PDD-63 high priority system, OIG strongly believes DCMWC is taking unnecessary risks in implementing their new system prior to assuring all identified issues have been resolved.

Recommendations

To minimize Black Lung data from exposure to risk of loss, misuse, or inadvertent/deliberate corruption, the OIG recommends the Assistant Secretary for ESA take the following actions:

- 1) DCMWC should take appropriate corrective action on the six high-risk management security control issues to eliminate or minimize the associated risks prior to rolling out the New ASP Black Lung System into production.
- 2) The 25 medium-risk management and technical security control issues identified should have appropriate corrective action taken in a timely manner.
- 3) In resolving recommendations 1 and 2 above, use a recognized comprehensive risk-based system certification and accreditation process.

INTRODUCTION AND BACKGROUND

Introduction

The U.S. Department of Labor's (DOL) Office of the Chief Information Officer (OCIO) issued on October 22, 1999, the Cyber Security Program Plan (CSPP), which places responsibility with the OIG to perform Security Testing and Evaluation (ST&E) Audits of DOL's PDD-63. The OIG tasked KPMG LLP the responsibility to perform an ST&E Pilot Audit on the New Automated Support Package (ASP) - Black Lung System.

This ST&E audit report presents observations, findings and recommendations related to specific security related areas, which were included in the audit's scope. The report provides an assessment of the areas covered under the audit and can be utilized as part of an overall system security certification process.

The findings and recommendations presented will aid DOL in the process of conducting a comprehensive risk-based Department-wide program to improve security under the CSPP process.

Background

DOL's Employment Standards Administration (ESA), Office of Workers' Compensation Programs (OWCP), Division of Coal Mine Workers' Compensation (DCMWC), and Federal Black Lung Program (FBLP) administers the Black Lung Benefits Act, as amended. This Act establishes a worker's compensation program to provide benefits to coal miners disabled by coal workers' pneumoconiosis (Black Lung disease). It also provides benefits to the eligible survivors of miners who died from or were disabled by coal workers' pneumoconiosis.

The FBLP serves approximately 150,000 active beneficiaries, including 13,000 Medical Benefit Only (MBO) beneficiaries, and operates an extensive medical bill payment system, with over 45,000 providers of medical services providing pulmonary care and treatment to its miner beneficiaries. DCMWC maintains extensive records regarding the status of the approximately 500,000 adjudicated claims. Under the program, eligible miners may receive monthly benefit payments and medical benefits for the treatment of coal workers' diseases. Dependent survivors of a deceased miner may also receive monthly benefit payments, but are not eligible for medical treatment benefits.

Applications are received and adjudicated, and eligible applicants are enrolled to receive benefits. Miners, having been found eligible for benefits, may submit requests (bills) for reimbursement of covered medical expenses. Alternatively, miners may go directly to health care providers for treatment under the program. The providers may then bill the Department of Labor directly, thereby avoiding an out-of-pocket expense for the miner.

The FBLP utilizes a computer system to support its mission in accounting of benefits and medical claims. The ASP provides support to the FBLP program. In general, the ASP tracks status, history, and location of claims for Black Lung benefits for the following business processes:

- paying monetary benefits
- paying medical expenses
- adjudicating medical necessity
- adjudicating benefit claims
- accounting related to the paying of benefits and claims
- claimant medical information
- general customer service activities

There are nine district offices and one national office where DCMWC staff and their support contractor Computer Science Corporation (CSC) perform the necessary data processing in order to serve the program claimants, beneficiaries, medical service providers and other interested parties. CSC provides DCMWC Contractor Support and Training Specialists, Data Transcriber, and Mail and File Clerk staff.

The current Black Lung application currently resides on a mainframe computer located in Norwich, Connecticut, and is managed by CSC, under an agreement with DOL. DOL and CSC are in the process of migrating the mainframe application to a client server version. The primary business functionality of the application will not change once the client server version is implemented. The main purpose of the migration is to enable an enhanced ability to automate many of the Black Lung processes performed by the DOL and the CSC staff in order to aid the Black Lung participants by providing more efficient processing of benefits, claims and inquiries.

The hardware and software, which will support the New ASP Black Lung system, include two Sequent SE-30 Servers (one will be used for production and the other for testing/development). The server's operating system utilizes the DYNIX operating system. The Sequent servers will be utilized for accessing/storing of the FBLP data. Once implemented, national and district office users will gain access to the New ASP Black Lung System, via their Local Area Network (LAN). The planned date for the implementation of the New ASP Black Lung System was not definitively set during our fieldwork audit period.

CHAPTER I - POSITIVE SECURITY CONTROL AUDIT OBSERVATIONS

During the course of our audit, we identified numerous positive security related areas of the New ASP Black Lung System and its supporting FBLP network. These positive security control areas, which follow, will aid the FBLP in mitigating some of the associated risks to Black Lung data.

- The audit team was successfully prevented in securing access to the FBLP's two Sequent SE30 Informix database servers, which use the DYNIX version of the Unix Operating System. The new client server versions of the Black Lung databases will reside on these servers.
- The audit's external scans of FBLP's Internet accessible network devices did not identify potential vulnerabilities on the FBLP's network. No vulnerabilities were identified for the DOL ESA firewall or devices that can be used to connect to the FBLP network via Internet access. ESA maintains firewalls and other filters to prevent unauthorized users from accessing the FBLP LAN/WAN system.
- External scans conducted on the Internet Protocol (IP) addresses for the ESA National Office LAN/WAN and FBLP Lanham and District Office LANs were unsuccessful in gathering information on reachable hosts on the scanned address spaces, including responding ports, detected services, and operating systems. All scans that were attempted indicate that hosts on the FBLP LAN/WAN are designated as "internal only" addresses and cannot be routed across the Internet.
- The Informix database system changes are properly documented and controlled.
- UNIX root user access appears to be adequate. Users are required to enter a secondary user ID and password that uniquely identifies the user granted root privileges.
- Password-cracking tool (John the Ripper v1.5) will be used by FBLP to monitor future the use of weak UNIX passwords.
- The system development life cycle procedures described in CSC's Digital System Development Methodology (DSDM) document appear adequate. CSC has adhered to the guidelines described in the DSDM for the development of the New ASP client-server application.
- The access to the FBLP (Lanham, Maryland) facility is adequately secured. An audit team member without a valid ID and purpose to gain access to the facility was denied access.
- CSC plans to schedule periodic independent security assessments of the client-server environment once the New ASP Black Lung System is in production.

- Network resources (file server, concentrators) are adequately monitored on a periodic basis for network performance and availability.
- The changes to the Microsoft NT network environment appear to be adequately controlled and documented.
- There were three medium-risk technical security control issues identified during the December 5, 2000, initial scanning of the New ASP Black Lung System and its supporting network operating system. These issues included the following:
 - Default administrator accounts have not been renamed for the FBLP's Novell and NT servers (admin and administrator).
 - Twelve administrative accounts are present on the FBLP network.
 - Anonymous log-on users are able to list domain names and enumerate share names (null session vulnerability).

DCMWC management agreed with the three medium-risk technical security control issues, as described above. DCMWC developed a plan of action to resolve these issues identified. On January 11, 2001, the audit team verified, during confirmation testing, that these three issues were appropriately corrected by DCMWC, therefore, they were not included in the technical security control issues in Finding 2 – Section D.

CHAPTER II – FINDINGS AND RECOMMENDATIONS

The identified management and technical security control issues are divided into two main findings:

- **High-Risk Management Security Control Issues**
- **Medium-Risk Management and Technical Security Control Issues**

Finding 1: High-Risk Management Security Control Issues
--

We have identified the following six high-risk management security control issues:

1. The FBLP – Black Lung System Security Plan (SSP) has not been finalized.
2. A contingency plan has not yet been drafted for the New Black Lung System.
3. Client-server security procedures for monitoring and auditing have not been formally documented.
4. Standards are not fully documented for determining access rights to security screens within the New ASP Black Lung System application.
5. Procedures have not been established for reviewing the ASP audit documentation: Security Transaction Audit Table and Security Transaction Audit Report.
6. Procedures are currently still under development to monitor/audit the UNIX environment on a periodic basis once the ASP application goes into production.

Each issue listed has been compared to the following applicable Federal criteria or guidelines: The Office of Management and Budget (OMB) Circular A-130, Appendix III, the 1987 Computer Security Act, the National Institute of Standards and Technology (NIST) – Generally Accepted Principles and Practices for Securing Information Technology Systems (Series 800-14) and Critical Infrastructure Assurance Office (CIAO) – Vulnerability Assessment Framework 1.1.

The audit team communicated the preliminary high-risk management control issues to DCMWC on December 11, 2000, and on January 24, 2001. DCMWC provided written responses to many of the management and technical security issues, which included a plan of action to resolve many of the issues in conjunction with the New ASP Black Lung System implementation. The high-risk management security control issues are provided in the following table.

High-Risk Management Security Control Issues

No.	High-Risk Management Security Control Issues	Criteria
1.	<p>The FBLP – Black Lung System Security Plan (SSP) has not been finalized. DCMWC has received comments from the OCIO on the SSP, however, they are not planning on making any revisions until after the New ASP System has been implemented. The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned. The system security plan should delineate the responsibilities and expected behavior of all individuals who will access the New Black Lung System. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for the New Black Lung System. The lack of an adequate system security plan may place the Black Lung data at risk from exposure of loss, misuse, or inadvertent/deliberate corruption.</p>	OMB A-130 Appendix III
	<p>Management response during fieldwork: On February 13, 2001, DCMWC stated that upon an agreement with the DOL’s Office of Chief Information Officer (OCIO), DCMWC will provide the OCIO an updated version of the New ASP Black Lung SSP by February 20, 2001.</p>	
	<p>A contingency plan has not yet been drafted for the New Black Lung System. Contingency</p>	OMB A-130 Appendix III

No.	High-Risk Management Security Control Issues	Criteria
2.	<p>planning directly supports an organization's goal of continued operations. Organizations should practice contingency planning because it makes good business sense. Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. The lack of an adequate contingency plan for the New ASP Black Lung System may cause the FBLP's critical functions and data not to be available to the beneficiaries and to system users in the event of system disruptions.</p>	
	<p>Management response during fieldwork: DCMWC states that the contingency plan will be updated in conjunction with implementation of the New ASP Black Lung System.</p>	
3.	<p>Client-server security procedures for monitoring and auditing have not been formally documented. Audit trails maintain a record of network processes and user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Without appropriate review of the monitoring and audit trails, known network software problems, violation of requirements by a user, or some unexplained network or user problem may go undetected.</p>	<p>NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems</p>
	<p>Management response during fieldwork: The client-server security procedures documentation for monitoring and auditing will be finalized with system implementation. DCMWC responded that during the first 3 months of operation, system reports and logs will be monitored at least once a week and more often, if warranted.</p>	

No.	High-Risk Management Security Control Issues	Criteria
4.	<p>Standards are not fully documented for determining access rights to security screens within the New ASP Black Lung System application. Logical access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Logical access controls can prescribe who or what is to have access to a specific application resource, but also the type of access that is permitted. Without fully documented access rights to the New ASP Black Lung data, the risk is present that individual system users, without a need to know a particular data set, may gain access to sensitive beneficiary records and plan data.</p>	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	<p>Management response during fieldwork: DCMWC will document these procedures in conjunction with the system implementation.</p>	
5.	<p>Procedures have not been established for reviewing the ASP audit documentation: Security Transaction Audit Table and Security Transaction Audit Report. Audit trails maintain a record of activity of application processes and user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails should be reviewed periodically. Without appropriate application-level administrator review of the audit trails, known application software problems, violation of requirements by a user, or some unexplained application or user problem, may go undetected.</p>	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	<p>Management response during fieldwork: Procedures will be developed in conjunction with system implementation. During the first 3 months of operation, system reports and logs will be monitored at least once a week or more often, if warranted.</p>	

No.	High-Risk Management Security Control Issues	Criteria
6.	<p>Procedures are currently still under development to monitor/audit the UNIX environment on a periodic basis once the ASP application goes into production. Audit trails maintain a record of system activity and user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Without appropriate system-level administrator review of the audit trails, known system software problems, violation of requirements by a user, or some unexplained system or user problem, may go undetected.</p>	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	<p>Management response during fieldwork: Procedures will be developed in conjunction with system implementation. During the first 3 months of operation, system reports and logs will be monitored at least once a week or more often, if warranted.</p>	

Conclusion

These six management security issues are high-risk because they would have the potential effect of increasing the risks of unnecessary system downtime, misuse and destruction/exposure of critical Black Lung data. DCMWC indicated it is continually addressing the six high-risk management control issues identified in the report, however, it appears that two of the issues will not be implemented prior to the April 9, 2001 roll-out date of the New ASP Black Lung System. To emphasize, the System Security Plan and Contingency Plan need to be completed and approvals obtained from the system owner and the Chief Information Officer prior to implementation to minimize the Black Lung data from exposure to risk of loss, misuse, or inadvertent/deliberate corruption, as these provide a foundation to implementing and maintaining any system securely. Additionally, there is the additional potential risk of the FBLP computer operations staff's time being occupied with addressing production issues of the New ASP Black Lung System once it goes live, thereby preventing these high-risk security issues from being resolved.

Using a comprehensive security certification and accreditation process, while implementing the New ASP Black Lung System, is the prudent way to address the impact of the six high-risk issues identified in this finding. The security certification and accreditation

process is a form of quality control for computer security of sensitive applications. In the area of system certification, Office of Management and Budget (OMB) Circular A-130 Appendix III, Section 3 – Review of Security Controls) states:

- i. . . . *In addition, periodic review of controls should also contribute to future authorizations. Some agencies perform ‘certification reviews’ of their systems periodically. These formal technical evaluations lead management accreditation, or ‘authorization process.’ Such certifications (such as those using the methodology in FIPS Pub 102 ‘Guideline for Computer Security Certification and Accreditation’) can provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan required by this [sic] Appendix.*

Security certification is a technical evaluation for the purpose of accreditation, and uses security requirements as the criteria for that evaluation. Security accreditation is management’s approval for operation, and is based on the technical evaluation and other management considerations. It should be noted that computer security certification and accreditation are one aspect of a general certification and accreditation activity that should be performed to assure that a computer system satisfies all its defined requirements.

It should be noted that management’s response to the Draft Report was not fully accurate when stating that, “the audit team could not penetrate either the network or the database servers...”. While it is true the audit team was unable to gain access to the database servers and to the FBLP network from an external perspective, we were, however, successful in securing complete and controlling access to all of the network’s NT and Novell Servers when probed from the within FBLP network.

Recommendations

To minimize Black Lung data from exposure to risk of loss, misuse, or inadvertent/deliberate corruption, the OIG recommends the Assistant Secretary for ESA take the following actions:

1. DCMWC should take appropriate corrective action on these six high-risk management security control issues to eliminate or minimize the associated risks prior to rolling out the New ASP Black Lung System into production.
2. In resolving the recommendation above, use a recognized comprehensive risk-based system certification and accreditation process.

Finding 2: Medium-risk management and technical security control issues

We identified 25 medium risk management and technical security control issues identified, which are related to the New ASP Black Lung System, FBLP's current operating environment, and the DCMWC district office sites.

These issues are broken out into four main areas:

- A. Medium-risk management security control issues related to the New ASP Black Lung System - 7 issues identified**
- B. Medium-risk management security control issues related to the current FBLP operating environment – 7 issues identified**
- C. Medium-risk management security control issues related to the DCMWC's district office sites – 6 issues identified**
- D. Medium-risk technical security control issues related to the current FBLP network environment – 5 issues identified**

It is important for DCMWC management to take appropriate corrective action on these 25 medium-risk security control issues in order to protect the integrity, availability, and confidentiality of Black Lung data.

Each condition listed has been compared to the following applicable federal criteria or guidelines: The Office of Management and Budget (OMB) Circular A-130, Appendix III, the 1987 Computer Security Act, the National Institute of Standards and Technology (NIST) – Generally Accepted Principles Practices for Securing Information Technology Systems (Series 800-14) and Critical Infrastructure Assurance Office (CIAO) – Vulnerability Assessment Framework 1.1.

The audit team communicated to DCMWC, the preliminary medium-risk management security control issues on December 11, 2000, and on January 24, 2001. DCMWC management concurred with many of the identified security control issues. Further, DCMWC

provided written responses to many of the management and technical security issues, which included a plan of action to resolve many of the issues in conjunction with the New ASP Black Lung System implementation. The medium-risk management security control issues are provided in the tables A, B and C, which follow.

A. Medium-risk management security control issues related to the New ASP Black Lung System

No.	A. Medium-risk management security control issues related to the New ASP Black Lung System	Criteria
1.	Security awareness training did not include FBLP’s policy against file sharing via the network neighborhood.	OMB A-130 Appendix III
	Management response during fieldwork: Security training has since been conducted as part of the client-server training sessions and included a section devoted to this issue. DCMWC also states that all users have been made aware of this policy.	
2.	An excessive number of employees have access to the data center, but this may be appropriate due to the current development environment. However, once the application is in production, FBLP should reevaluate personnel with access to the data center.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: The access list to the data center is reviewed on a routine basis. Personnel who no longer require access to the data center are removed from the access list.	

No.	A. Medium-risk management security control issues related to the New ASP Black Lung System	Criteria
3.	The current segregation of duties within the FBLP appears to be adequate. We are aware that due to system testing, user access rights to particular application security screens are not finalized.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: DCMWC officials stated that a final check of the system users' access rights has been identified as a necessary activity prior to moving to production and has been included the client-server Project Management Plan (PMP) for over a year. It has also been identified and included in the client-server implementation plan.	
4.	Logical access controls over the Informix database appear appropriate; however, criteria have not been established to determine how RESOURCE and DBA level access will be granted once the ASP application is in production.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: In conjunction with system implementation, the criteria will be established for logical access controls over the Informix database. Once this has been determined, the access will be evaluated for the client-server list of appropriate individuals. This will be established and documented in the Technical Services Standards and Procedures (TSSP).	

No.	A. Medium-risk management security control issues related to the New ASP Black Lung System	Criteria
5.	Access to the development instances of the New ASP application has been appropriately granted during the development stage. While current RESOURCE and DBA access is appropriate for the development stage, this can cause potential security weaknesses if not timely updated.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: In conjunction with system implementation, the RESOURCE and DBA access to the production instance will be reviewed with the client and the criteria for the access will be documented in the TSSP. The access to production will then be evaluated and continually updated as necessary.	
6.	Full UNIX shell access has been granted under the current development environment. However, once the New ASP goes into production, full shell access should be revoked for non-essential Testing, Software Development, Data Administration, DOL Project Team, and Network Services personnel.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response fieldwork: The listing of personnel with UNIX shell access is reviewed on a routine basis. Personnel who no longer require shell access are removed.	

No.	A. Medium-risk management security control issues related to the New ASP Black Lung System	Criteria
7.	The configuration and change management procedures for the New ASP software have not been finalized. The procedures are currently in draft form and are based upon mainframe change management procedures found in the Hardware Configuration Handbook (HCMH), Software Configuration Handbook (SCMH) and Technical Service Standards and Procedures (TSSP) documentation. The HCMH, SCMH and TSSP are scheduled for revision to incorporate the change from a mainframe to a client-server environment.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: The procedures will be updated and tracked in accordance with the Configuration Control Board's (CCB) Enhancement Request (ER) process. Documentation updates are scheduled for completion after client-server implementation. These procedures will mirror currently used mainframe configuration management processes.	

B. Medium-risk management security control issues related to the current FBLP operating environment

No.	B. Medium-risk management security control issues related to the current FBLP operating environment	Criteria Cited
1.	FBLP does not consistently utilize screen-saver technology on PCs connected to the LAN. The audit team was able to successfully gain access to seven unattended PCs and send e-mails from the users' mail accounts.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: DCMWC will evaluate this suggestion and will implement if feasible.	
2.	Visitors to the computer room are not required to sign a visitor's log.	Critical Infrastructure Assurance Office (CIAO) – Vulnerability Assessment Framework
	Management response during fieldwork: A visitor log has been implemented for the computer room.	

No.	B. Medium-risk management security control issues related to the current FBLP operating environment	Criteria Cited
3.	The auditing functionality (e.g., – excessive log-on attempts) of the Novell network is disabled. The audit team recommends that certain auditing functionalities be reviewed to identify if they can be implemented without overly taxing system resources.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: The audit function of Netware is extremely resource intensive and would have an impact on FBLP network performance. In regards to the client-server, access to the Netware network could only allow an intruder to access the FBLP network and does not provide access to the Sequent equipment. The application would be further controlled by the application’s Security Master application code. Auditor’s Note: While it is true that the Sequent application has its own access control process, the risk is still present that the Novell network could be compromised or made unavailable, thereby preventing the FBLP users access to the application. In addition, the Novell monitoring/logging tool allows the system administrator to turn on/off specific logging commands, thereby minimizing the potential resource drain on the FBLP network performance.	
4.	There are no procedures in place to periodically review the network neighborhood to ensure file and drive sharing does not occur.	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	Management response during fieldwork: File and drive sharing is being addressed in the client-server security procedures. This document will be finalized following implementation.	

No.	B. Medium-risk management security control issues related to the current FBLP operating environment	Criteria Cited
5.	Network change control procedures (upgrades, software patches, configuration settings) are currently still being revised to provide a uniform network change control process for the FBLP Novell and NT network environments.	Critical Infrastructure Assurance Office (CIAO) – Vulnerability Assessment Framework
	Management response during fieldwork: These procedures will be finalized in conjunction with implementation.	
6.	Procedures are currently being developed for periodic reviews of the FBLP network using Internet Security Scanner (ISS). DCMWC plans on having ISS reports reviewed and submitted to DOL on a monthly basis.	OMB A-130 Appendix III
	Management response during fieldwork: Procedures for these reviews will be finalized in conjunction with implementation. The FBLP security team reviews the ISS reports on a monthly basis. The results are shared with appropriate platform security personnel for risk assessment and mitigation. Documentation will be developed and/or finalized in conjunction with implementation.	
7.	Novell network change documentation does not include the person(s) responsible for network changes. Furthermore, management approval for each network change is not documented. The documentation does not include information indicating that the network changes were verified to ensure proper function of the network after the changes were made.	Critical Infrastructure Assurance Office (CIAO) – Vulnerability Assessment Framework
	Management response during fieldwork: The change control process utilized on the NT platform has been implemented on the Novell Netware platforms.	

C. Medium-risk management security control issues related to the DCMWC’s district office sites

No.	C. Medium-risk management security control issues related to the DCMWC’s district office sites	Criteria Cited
1 and 2	<p>Issues identified at both the Johnstown and Greensburg District Offices:</p> <ul style="list-style-type: none"> • Wet-pipe fire sprinkler systems in/near the area of the network computer equipment. • Updated DOL Security Awareness Training has not been conducted. 	<p>NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems</p> <p>OMB A-130 – Appendix III</p>
	<p>Management response during fieldwork: Security Awareness Training has recently been conducted as part of the client server training. Auditor’s Note: There was no management response to the Water-based fire sprinkler systems in/near the area of the network computer equipment condition. The audit team recommends that management consider updating the fire suppression equipment and install a dry-pipe fire suppression system such as CO₂ or FM200. The potential effect of the continued use of wet-pipe fire suppression, is if there is an accidental/actual activation of the fire suppression system, which could result in the damage of the district offices’ network computer equipment, thereby preventing the District Office users to be able to access Black Lung Data.</p>	

No.	C. Medium-risk management security control issues related to the DCMWC's district office sites	Criteria Cited
3	<p>The following issue was identified at the Johnstown Office only:</p> <ul style="list-style-type: none"> • The front-door cipher-locks are not changed on a regular basis or after an employee terminates employment. 	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	<p>Management response during fieldwork: DCMWC will revise the procedures to resolve this problem.</p>	
4, 5, and 6	<p>The following issues were identified at the Greensburg Office only:</p> <ul style="list-style-type: none"> • The Greensburg District Office Computer Equipment is located out in the open of the office, and its wires are exposed to potential unplugging and other unforeseen acts which may cause the District's connection to the Black Lung network inoperable. • There were no visitor badges required. • There appeared to be a lack of enforcement of the sign-out log. Upon observation of the sign-out log, it appears that previous day visitors were not required to sign-out for the time they left the facility. 	NIST 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
	<p>Management response during fieldwork: DCMWC will review these conditions.</p>	

D. Medium-risk technical security control issues related to the current FBLP network environment

This portion of our assessment was limited to FBLP's internal systems and network. The FBLP internal network consists of Novell, Windows NT, and Unix servers, with a NT-based Primary Domain Controller (PDC) and Backup Domain Controller (BDC), Novell application/file/print servers, Novell mail servers, NT imaging and Intranet servers, Unix client/server databases and Network Management Station and, and user workstations.

The following key areas of vulnerability were identified for the NT and Novell Servers:

- Password Management
- System Configuration

The audit team communicated to DCMWC, the preliminary medium-risk technical control issues on December 11, 2000, and on January 24, 2001. DCMWC management concurred with many of the identified security control issues. Further, DCMWC provided written responses to many of the technical security issues, which included a plan of action to resolve many of the issues. A few of the technical security issues identified during the initial December 5, 2000 test were resolved by FBLP computer operations staff (see Positive Security Control Audit Observations section). It should be noted that not all of the DCMWC's responses and actions to the issues identified were verified by the audit team because the management responses were provided after the completion of fieldwork. The five medium-risk technical security control issues are provided in the tables below.

Password Management

No.	D. Medium-risk technical security control issues	Criteria Cited
1	A password filter is not implemented on the FBLP network to enforce strong passwords (passwords containing at least three of the following: lowercase letters, uppercase letters, numbers, and special or non-numeric characters).	OMB Circular A-130 Appendix III
	<p>Management response during fieldwork: Pandora will be run every 30-90 days to crack Novell passwords. Users will be forced to change weak passwords immediately. DOL will be notified of this implementation date as soon as CSC assesses the work effort to implement the use of the Pandora tool in this fashion.</p> <p>NT passwords filters that follow this guideline (passwords containing at least three of the following: lowercase letters, uppercase letters, numbers, and special or non-numeric characters) will be instituted.</p> <p>DCMWC has instructed users to use strong passwords. Additionally, this topic was covered during the security portion of training on the new client sever system. DCMWC system support contractor, Computer Science Corporation, has incorporated the use of L0phtCrack on a monthly basis to ensure that strong passwords are utilized</p>	

No.	D. Medium-risk technical security control issues	Criteria Cited
2	All passwords on four FBLP NT servers (including the Primary Domain Controller) and two FBLP Novell servers were successfully guessed by KPMG's password cracking utility.	OMB Circular A-130 Appendix III
	<p>Management response during fieldwork: IDL and NCP Packet Signature Option Level 3 have been implemented for Novell.</p> <p>NT passwords filters that follow this guideline (passwords containing at least 3 of the following: lowercase letters, uppercase letters, numbers, and special or non-numeric characters) will be instituted. DCMWC has instructed users to use strong passwords. Additionally, this topic was covered during the security portion of training on the new client sever system. DCMWC system support contractor, Computer Science Corporation, has incorporated the use of L0phtCrack on a monthly basis to ensure that strong passwords are utilized.</p>	

No.	D. Medium-risk technical security control issues	Criteria Cited																		
3	<p>Password aging on Domain Administrator accounts has not been implemented. The table provided below lists the domain accounts where passwords have not been changed on a regular basis.</p> <table border="1" data-bbox="382 477 1541 967"> <thead> <tr> <th data-bbox="388 482 1066 548">Domain Account</th> <th data-bbox="1073 482 1535 548">Number of days since last password change</th> </tr> </thead> <tbody> <tr> <td data-bbox="388 553 1066 591">Managexec (Seagate Management Account)</td> <td data-bbox="1073 553 1535 591">500</td> </tr> <tr> <td data-bbox="388 596 1066 633">Managexec1 (Seagate Management Account)</td> <td data-bbox="1073 596 1535 633">429</td> </tr> <tr> <td data-bbox="388 638 1066 675">IUSR_BLWEB (Internet Guest Account)</td> <td data-bbox="1073 638 1535 675">464</td> </tr> <tr> <td data-bbox="388 680 1066 717">IUSR_BLWEB2 (Internet Guest Account)</td> <td data-bbox="1073 680 1535 717">821</td> </tr> <tr> <td data-bbox="388 722 1066 760">IUSR_FBLP_INTDB1 (Internet Guest Account)</td> <td data-bbox="1073 722 1535 760">687</td> </tr> <tr> <td data-bbox="388 764 1066 802">IWAM_BLWEB (Web Application Manager)</td> <td data-bbox="1073 764 1535 802">821</td> </tr> <tr> <td data-bbox="388 807 1066 844">IWAM_BLWEB2 (Web Application Manager)</td> <td data-bbox="1073 807 1535 844">821</td> </tr> <tr> <td data-bbox="388 849 1066 963">OZTAKUN1271</td> <td data-bbox="1073 849 1535 963">Was re-set between December 5, 2000 and January 11, 2001 tests, however, password is currently configured never to expire.</td> </tr> </tbody> </table>	Domain Account	Number of days since last password change	Managexec (Seagate Management Account)	500	Managexec1 (Seagate Management Account)	429	IUSR_BLWEB (Internet Guest Account)	464	IUSR_BLWEB2 (Internet Guest Account)	821	IUSR_FBLP_INTDB1 (Internet Guest Account)	687	IWAM_BLWEB (Web Application Manager)	821	IWAM_BLWEB2 (Web Application Manager)	821	OZTAKUN1271	Was re-set between December 5, 2000 and January 11, 2001 tests, however, password is currently configured never to expire.	OMB Circular A-130 Appendix III
Domain Account	Number of days since last password change																			
Managexec (Seagate Management Account)	500																			
Managexec1 (Seagate Management Account)	429																			
IUSR_BLWEB (Internet Guest Account)	464																			
IUSR_BLWEB2 (Internet Guest Account)	821																			
IUSR_FBLP_INTDB1 (Internet Guest Account)	687																			
IWAM_BLWEB (Web Application Manager)	821																			
IWAM_BLWEB2 (Web Application Manager)	821																			
OZTAKUN1271	Was re-set between December 5, 2000 and January 11, 2001 tests, however, password is currently configured never to expire.																			
	Management response during fieldwork: Password aging has been implemented on the identified accounts.																			

OMB Circular A-130 states that agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Technical and operational controls support management controls. To be effective, all must interrelate. For example, authentication of individual users is an important management control, for which

password protection is a technical control. However, password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly.

The vulnerabilities identified for password management exist due to the lack of adequate access control policies and procedures in the areas of password filtering, encryption, aging, and user awareness.

Without proper control of passwords, the potential exists for an unauthorized user to gain access to the system. Active accounts with guessable passwords provide an easy point of entry for attackers. This could result in unnecessary system downtime and potential loss, misuse and destruction/exposure of critical Black Lung data on the FBLP LAN/WAN.

The password practices to log on to the FBLP network should be strengthened to prevent “door knocking” penetration of user accounts, in which an intruder attempts to log on as an authorized user. All accounts that report vulnerable to the ‘Guessable NetBIOS/SMB password’ check should be secured immediately through the use of password filtering. Password cracking utilities are recommended to crack weak passwords on Novell and NT servers. Also, the server parameters for password expiration should be set for a maximum of 45 to 90 days.

System Configuration

No.	D. Medium-risk technical security control issues	Criteria cited
4	The Web Server Folder Traversal Vulnerability exists on the FBLP's Microsoft Internet Information Server (IIS) web servers. This vulnerability involves a serious flaw in the IIS UNICODE translation and is extremely simple to exploit. It gives the attacker the ability to break out of the web server root directory, access and manipulate files in other locations, and execute arbitrary commands.	OMB Circular A-130 Appendix III
	Management response during fieldwork: DCMWC/CSC has installed the patch as identified in the Microsoft security bulletin to eliminate the vulnerability.	

No.	D. Medium-risk technical security control issues	Criteria cited
5	The Remote Database Services (RDS) Vulnerability exists on FBLP's web servers operating under Windows NT 4.0. This vulnerability allows an attacker on the Internet to run arbitrary commands with System level privileges or manipulate data on the FBLP web servers.	OMB Circular A-130 Appendix III
	Management response during fieldwork: DCMWC has removed three registry keys to eliminate the vulnerability per Microsoft security bulletin.	

The Department of Labor CSPP states that “agencies are responsible for hardware/software inventories as well as downloading, testing, and installing patches.” OMB Circular A-123 states, “Access and Accountability for Resources. Access to resources and records should be limited to authorized individuals, and accountability for the custody and use of resources should be assigned and maintained.” Furthermore, implementation of technical, operational and management controls are mandated by OMB Circular A-130 to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems.

The web server vulnerabilities resulted since current security patches, such as the UNICODE vulnerability patch, are not downloaded, installed, and applied to the FBLP Web Server. NT Registry keys are also incorrectly configured to prevent the RDS vulnerability. Vulnerabilities such as the Web Server Folder (UNICODE Directory) Traversal vulnerability and RDS vulnerability could potentially be exploited and lead to the compromise of the entire FBLP LAN/WAN network and affect the availability, confidentiality, and integrity of FBLP data. To ensure the integrity of FBLP data, the appropriate patches for the Web Server Folder Traversal vulnerability should be downloaded from Microsoft’s web site and applied to the FBLP web server. Applicable registry keys should be removed to eliminate the RDS vulnerability.

Conclusion

These 25 medium-risk management security control issues identified, are related to the New ASP Black Lung System, FBLP's current operating environment, and the DCMWC district office sites. DCMWC indicated in its March 27, 2001 response to the draft audit report that it has addressed all but two of the issues – password protected screen savers and dry-pipe fire suppression for the District Offices. Management will evaluate the feasibility of resolving these issues in the future. It is important for DCMWC management to assure that appropriate corrective action has been taken on these 25 medium-risk security control issues in order to protect the integrity, availability, and confidentiality of Black Lung data.

Using a comprehensive security certification and accreditation process prior to implementation, and during operations, is the prudent way to address the impact of the 25 medium risk issues identified in this finding. The security certification and accreditation process is a form of quality control for computer security of sensitive applications. In the area of system certification, Office of Management and Budget (OMB) Circular A-130 Appendix III, Section 3 – Review of Security Controls) states:

- ii. . . . *In addition, periodic review of controls should also contribute to future authorizations. Some agencies perform 'certification reviews' of their systems periodically. These formal technical evaluations lead management accreditation, or 'authorization process.' Such certifications (such as those using the methodology in FIPS Pub 102 'Guideline for Computer Security Certification and Accreditation') can provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan required by this [sic] Appendix.*

Security certification is a technical evaluation for the purpose of accreditation, and uses security requirements as the criteria for that evaluation. Security accreditation is management's approval for operation, and is based on the technical evaluation and other management considerations. It should be noted that computer security certification and accreditation are one aspect of a general certification and accreditation activity that should be performed to assure that a computer system satisfies all its defined requirements.

It should be also noted that the Novell monitoring/logging tool allows the system administrator to turn on/off specific logging commands, thereby minimizing the potential resource drain on the FBLP network performance. While it is true that the Sequent application has its own access control process, the risk is still present that the Novell network could be compromised or made unavailable, thereby preventing the FBLP users access to the application.

Recommendations

To minimize Black Lung data from exposure to risk, the OIG recommends the Assistant Secretary for ESA take the following actions in order to protect the integrity, availability, and confidentiality of Black Lung data.

- 1) The 25 medium-risk management and technical security control issues identified should have appropriate corrective action taken in a timely manner.
- 2) In resolving the recommendation above, use a recognized comprehensive risk-based system certification and accreditation process.

OBJECTIVES, SCOPE AND METHODOLOGY

Objectives

The objectives of the ST&E were to determine whether the security controls, when compared to applicable Federal guidelines, over the New ASP Black Lung and its supporting network environment will sufficiently protect the Black Lung data. The emphasis of the audit was to examine the New ASP, which at the time of the audit was in the implementation phase; however, many the audit steps assessed controls, which were still in the design phase. Many of the findings included in this audit report will be from the perspective of control issues, which we recommend that appropriate corrective action be taken prior to implementing the New ASP Black Lung System.

The objectives of the ST&E were divided into two primary areas:

- Management security controls
- Technical security controls

The management security controls of the review were as follows:

- a) Conduct a high-level risk assessment of the New ASP Black Lung System within each of the security control areas:
 - Entity-wide security
 - Logical and physical access
 - Segregation of duties
 - Change control and life cycle management
- b) Review and test the installation and configuration of the New ASP System network operating system - Local Area Network (LAN), and Wide Area Network (WAN)
- c) Validate results of assessments with the appropriate management and system administrators to determine whether there are appropriate compensating controls to mitigate conditions found.

The technical security controls of the review included:

- a) Identify and document the technical systems architecture for the New ASP Black Lung system.

- b) Review and test the technical security controls by scanning the New ASP Black Lung System and its supporting network operating system to identify vulnerabilities in Federal Black Lung Program's (FBLP) network environment which could be potentially exploited to gain unauthorized access to Black Lung data.
- c) Validate results of assessments with the appropriate management and system administrators to determine whether there are appropriate compensating controls mitigate conditions found.

Scope

We performed the ST&E audit on the New ASP Black Lung System to evaluate the identified security controls to applicable Federal guidelines. An ST&E audit involves finding and documenting the vulnerabilities in critical information assets. The audit process examined the adequacy of the FBLP's areas of control, either in place or planned to be in place, in order to measure the organization's effectiveness in protecting the Black Lung data. The results of the audit will aid in the identification of areas of potential compromise, which provides for a comprehensive list of vulnerabilities for which additional security measures, and/or modifications/updates to security policy may be necessary prior to implementation.

The scope of our management security control assessment considered the New ASP Black Lung System, its supporting network environment, and the controls in place at the FBLP's district office locations.

The scope of our technical assessment considered all critical information technology devices connected to the FBLP network. Specifically, the external portion of this vulnerability assessment focused on the local area network/wide area network (LAN/WAN) connection that provides the only interface for the FBLP network to the Internet. This interface through the Employment Standards Administration (ESA) network is managed by the Division of Information Technology Management and Services (DITMS).

The internal portion of this vulnerability assessment was limited to the LAN supporting FBLP's Lanham, Maryland, site. The focus was placed on particular network servers (NT and Novell) after it was demonstrated that a complete mapping of the site's network topology and scanning could be conducted by an unauthorized individual without insider knowledge.

Details regarding the FBLP network devices and technology included in this assessment are provided in the table that follows:

Network Device	Primary Function	Operating Software
Firewall	Internet firewall (ESA)	Checkpoint
Routers	Routers for FBLP network traffic (ESA and FBLP)	Cisco
Novell servers	FBLP e-mail/SMTP gateway, file and print support for FBLP development and production environment	Novell 4.11
Windows NT servers	FBLP Imaging System, Intranet and Web services	Windows NT 4.0
Sequent Servers	FBLP Client/Server Databases	DYNIX
Windows NT and 95 workstations	FBLP end user applications	Windows NT 4.0 and 95

The ST&E audit was performed in Washington D.C., Lanham, Maryland, and two DCMWC District Offices (Johnstown and Greensburg, Pennsylvania) from October 2000 through February 2001 in accordance with *Government Auditing Standards (GAS)*, issued by the Comptroller General of the United States.

We used the following criteria to perform our ST&E audit:

- Vulnerability Assessment Framework 1.1 - Critical Infrastructure Assurance Office (CIAO), October 1998.
- Computer Security Act of 1987 – Public Law 100 – 235, January 1988.
- Office of Management Budget Circular A-130, Appendix III, August 1996.
- An Introduction to Computer Security: The NIST Handbook – 800-12, National Institute of Standards and Technology, October 1995.
- Generally Accepted Principles and Practices for Securing Information Technology Systems – 800-14, National Institute of Standards and Technology, September 1996.
- Guide for Developing Security Plans for Information Technology Systems – 800-18, National Institute of Standards and Technology, December 1998.
- Practices for Securing Critical Information Assets – Critical Infrastructure Assurance Office (CIAO), January 2000.
- Guideline for Computer Security Certification and Accreditation – Federal Information Processing Standards Publication (FIPS) Publication Number 102, December 1983.

Methodology

Our methodology included assessing the control environment from many different perspectives. Our audit included reviewing technical controls in place, as well as, the management control areas, which also play a critical role in assuring that New ASP Black Lung System will have controls in place in order to protect the integrity, availability, and confidentiality of Black Lung data. The areas of control the audit focused on included the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that FBLP business objectives will be achieved and that undesired events will be prevented or detected and corrected in a timely manner.

The Audit of the Management Security Controls included the following steps:

Entity-wide security - Refers to planning and management that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and information system security controls. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

Physical and logical access controls - The procedures and controls that limit or detect access to critical asset resource elements (people, systems, applications, data and/or facilities) to guard against loss of integrity, confidentiality, accountability, and/or availability. Access controls provide reasonable assurance that resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. They may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

Segregation of duties - Entails policies, procedures, and an organizational structure established to ensure that no single individual controls multiple key aspects of physical and/or computer-related operations. Failure to segregate duties could allow someone to conduct unauthorized actions or gain unauthorized access to critical assets without detection. Segregation of duties is defined as the process of segregating work responsibilities to ensure critical stages of a process are not under the control of a single individual. This objective is achieved by dividing responsibilities for critical process stages between two or more individuals or groups. Dividing duties allows for the activities of one group or individual to serve as a check on the activities of the other and reduces the possibility that errors and wrongful acts will be committed and/or go undetected.

Change control and life cycle management - Procedures and controls prevent implementation of unauthorized programs or modifications to existing programs. Change control and life-cycle management policies provide reasonable assurance that changes to applications will not interrupt the critical processes. Life-cycle management policies guide software specifications, implementation, and testing. Change control policies govern application and system modifications for in-house and commercial packages or patches. An adequate set of policies, procedures, and techniques ensures that: (1) all program modifications are properly authorized, tested, and approved before implementation; and (2) access to and distribution of programs is carefully controlled.

The Audit of the Technical Security Controls included the following steps:

Our approach included a review of documentation supporting network operations, browsing the Internet to identify information about FBLP, and execution of logical network scans to identify potential vulnerabilities. Our approach was conducted from both an external (outside the network) perspective and an internal (inside the network) perspective.

External Assessment

Automated scans of network and modem devices attached to the FBLP network were performed to identify potential vulnerabilities.

- **Network Scans**

The external Internet penetration testing was conducted from the perspective of an outsider with no knowledge of DOL or FBLP's external web sites, topology or operations. The outsider would have no access to the physical site and no system access. Initially, the external assessment reviewed DOL's primary firewall and main web site in search of vulnerabilities that could potentially be exploited and lead to the compromise of the entire network supporting the Department of Labor, despite network security controls within the FBLP network.

Then, the focus of the external assessment shifted to the DOL ESA firewall or devices that can be used to connect to the FBLP network via Internet access. The final portion of the external scan specifically addressed the FLBP LAN/WAN network for the Lanham site and nine District Offices.

KPMG used a number of tools and scripts to identify vulnerabilities on DOL and FBLP hosts. The tools included NMAP, Internet Security Systems' Internet Scanner, and Network Associates' Cybercop Scanner.

- **War Dialing**

An automated telephone dialing (also known as war dialing) was conducted using the TeleSweep Secure software to identify FBLP desktop computers that were accessible through remote telephone dial-in. War dialing of FBLP telephone

numbers sought to discover telephones with active modems that were connected to computers to discover applications and services hosted on these computers.

Internal Assessment

The internal penetration testing was conducted from the perspective of a FBLP employee with physical access to the Lanham, Maryland, site in two scenarios:

- an employee with physical access to the site but who does not have access to system resources
- an employee with physical access to the site and access to system resources (i.e., a knowledgeable insider who has access to the FBLP local area network and the ability to employ hacker tools against the FBLP system)

Using a network connection assigned by a FBLP network administrator, access to the FBLP Lanham network segment was attempted. A combination of tools were deployed against the FBLP Internet Protocol (IP) addresses to identify vulnerabilities and confirm their validity. The following is a listing of the tools used in the testing:

- Hunt
- Hyena
- SuperScan
- Nessus
- Cerberus Web Scanner
- Network Associates, Inc. CyberCop
- Cisco NetSonar Security Scanner

GLOSSARY

BDC (Backup Domain Controller) -- A backup server that protects the integrity and availability of the Security Accounts Manager (SAM) database. BDCs are not able to make changes or modifications, but they can use the database to authenticate users.

Client/Server -- A distributed computing architecture that splits applications to allow a client (front-end desktops of the end users of PCs and workstations) to request services from a server (back-end network server).

Firewall -- A barrier (made of software and/or hardware) between two networks, permitting only authorized communication to pass.

Gateway -- The service performed by a computer that converts the protocols between different types of networks or computers.

Group -- Collections of users defined with a common name and level of resource permissions.

HTTP (HyperText Transfer Protocol) -- The World Wide Web protocol that allows for the transfer of Hypertext Markup Language (HTML) documents over the Internet or intranets and responds to actions (such as a user clicking on hypertext links).

IIS (Internet Information Server) -- Web server software by Microsoft that is included and implemented with Window NT Server.

Internet -- The collection of TCP/IP-based networks around the world.

IP (Internet Protocol) -- This protocol specifies the format of packets and the addressing schedule. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

ISS (Internet Security Scanner) - A software program used to conduct network vulnerability assessments and audit analysis.

LAN (Local Area Network) -- A group of computers and associated peripheral devices connected by a communications channel, capable of sharing files and other resources between several users.

NCP (NetWare Core Protocol) -- A Novell NetWare presentation-layer procedure used by a server when responding to workstation requests. It includes routines for manipulating directories and files, printing, and creating and destroying connections.

NetBIOS (Network Basic Input Output System) -- A network protocol, originally developed in the 1980s by IBM, to manage data exchange and network access. This protocol provides the underlying communication mechanism for some basic NT functions, such as browsing and interprocess communications between network servers.

PDC (Primary Domain Controller) -- The central storage and management servers for the Security Accounts Manager (SAM) database.

Permissions -- A level of access assigned to files or folders. Permissions determine who has access rights to those files or folders.

Registry -- The NT hierarchical database that serves as a repository for hardware, software, and operating system configuration information.

Rights -- Settings that define the ability of a user to access a computer or a domain.

Router -- A device or a software implementation that enables interoperability and communication across networks.

SAM (Security Accounts Manager) -- The security database of NT that maintains a record of all users, groups, and permissions within a domain. The SAM is stored on the PDC and is duplicated on the BDCs.

Share -- A network construct that enables remote users to access resources located throughout a network.

SMB (Server Message Block) -- A distributed file system network protocol, developed by Microsoft, which allows a computer to use the files and other resources of another computer as though they were local. For network transfers, SMBs are encapsulated within the NetBIOS network control block packet.

SMTP (Simple Mail Transport Protocol) -- The Internet protocol for sending e-mail messages between servers over a TCP/IP network. Also, SMTP is generally used to send messages from a mail client to a mail server.

TCP/IP (Transport Control Protocol/Internet Protocol) -- The most widely used protocol in networking, because it is the most flexible of the transport protocols and is able to span wide areas.

Unix -- An interactive time-sharing operating system developed in 1969 by a hacker to play games. This system developed into the most widely used industrial-strength computer operating system in the world, and ultimately, the birth of the Internet.

User account -- The collection of information, such as name, password, group memberships, access privileges, and user rights, stored by a network operating system (e.g., Novell, NT) about a specific network user.

WAN (Wide Area Network) -- A network that spans geographically distant segments. Often a distance of two or more miles is used to define a WAN.



Reply to the Attention of:

March 27, 2001

MEMORANDUM FOR JOHN J. GETEK

Assistant Inspector General
for Audit

FROM:

Anne L. Baird-Bridges
ANNE L. BAIRD-BRIDGES
Director, Office of Management,
Administration and Planning

SUBJECT:

Security Testing and Evaluation
Pilot Audit of the New Automated Support
Package (ASP) Black Lung System
OIG Draft Audit Report No. 17-01-003-04-433

This is in response to your March 6, 2001 memorandum addressed to Acting Assistant Secretary Joe Kennedy requesting comments on the subject report. We have reviewed the report and updated our response to the issues where necessary. Our comments are attached.

Attachment

U. S. Department of Labor
Office of Inspector General Audit

Security Testing and Evaluation
Pilot Audit of the New Automated Support
Package (ASP) Black Lung System
OIG Draft Audit Report No. 17-01-003-04-433

Employment Standards Administration Response to
OIG Findings and Recommendations

The audit examined the security policies and procedures attending the new client server system that will support DCMWC program operations. This system was not operational when the audit was conducted and the audit report drafted. At this time, the program has concluded acceptance testing and is in the process of converting data from the legacy mainframe system to the client server platform. The new system will be operational on April 9, 2001.

As noted in the executive summary, many "positive security control observations" were identified and many of the issues noted during the audit have already been resolved. Given the many positive findings and the absence of significant substantive security shortcomings, the report, taken as a whole, reflects the fact that the program has a strong security program in place for the new ASP system.

Positive Security Control Audit Observations

The Draft Report notes several "positive security control areas." Specifically, the audit team could not penetrate either the network or the database servers and could not gain access to the database, application or UNIX root user account. Additionally, the report notes that system life cycle development procedures are adequate and database system changes are properly documented and controlled. The report recognizes that fact that network resources are monitored on a periodic basis to ensure network performance and availability. The report also notes DCMWC plans for periodic independent security assessments of the system following implementation. Finally, while the report notes certain security "risks", these shortcomings generally relate to documentation rather than to actual policies or procedures and, as noted in the response below, have been addressed by the program. Given the extensive system, application and security testing that the program has conducted, the extensive and comprehensive planning and documentation, and the generally positive security audit, DCMWC is confident that the new client server system is ready for production. Accordingly, DCMWC plans to begin implementation of the client server system on March 28, 2001 and the system will be operational on April 9, 2001.

High-Risk Management Security Control Issues

1. The Federal Black Lung Program – Black Lung Application System Security Plan (SSP) has not been finalized.

Response: DCMWC believes that its security plan conforms to all of the substantive requirements established by the OCIO. OCIO objected to the formatting of the documentation. DCMWC will update the documentation to conform to OCIO requirements once the new system is implemented. On February 8, 2001, DCMWC discussed this approach with OCIO staff. The Draft report incorrectly states that “DCMWC will provide the OCIO an updated version of the New ASP Black Lung SSP by February 20, 2001.” In fact, DCWMC stated that “by February 20, DCMWC (will) provide a date by which the security plan documentation will be updated to conform with OCIO guidelines.” DCMWC subsequently complied with this request, indicating to the OCIO that a revised plan would be provided by April 20, 2001. The revised security plan, in the format requested by the OCIO, is currently in draft form and undergoing internal review by federal and contractor staff.

2. A contingency plan has not yet been drafted for the new Black Lung system.

Response: The existing DCMWC contingency plan has been updated and is undergoing internal review by federal and contractor staff.

3. Client-server security procedures for monitoring and auditing have not been formally documented.

Response: Procedures have been established for auditing network and user activity. Audit trails are available for all critical network and system functions. Documentation will be finalized in conjunction with system implementation. Additionally, interim procedures have been established that provide for careful oversight during the initial phase of operation. During the first three months of operation, system reports and logs will be monitored at least once a week and more often if warranted.

4. Standards are not fully documented for determining access rights to security screens within the New ASP Black Lung System application.

Response: Logical access controls are in place and are documented in the ASP security plan. This documentation has been updated to conform to OCIO requirements and is undergoing internal reviews by federal and contractor staff.

5. Procedures have not been established for reviewing the ASP audit documentation: Security Transaction Audit Table and Security Transaction Audit Report.

Response: Interim procedures have been developed. During the first three months of operation, system reports and logs will be monitored at least once a week and more often if warranted. Permanent procedures will be developed based on the experience of the first three months of operation. Documentation will be updated accordingly.

6. Procedures are currently still under development to monitor/audit the UNIX environment on a periodic basis once the ASP application goes into production.

Response: Procedures for monitoring the UNIX environment have been established. During the first three months of operation, system reports and logs will be monitored at least once a week and more often if warranted. Permanent procedures will be developed based on the experience of the first three months of operation. Documentation will be updated accordingly.

The draft report concludes this section by stating that "these six management security issues are high-risk because they would have the potential effect of increasing the risks of unnecessary system downtime, misuse and destruction/exposure of critical Black Lung data. If DCMWC does not take appropriate corrective action of these six high-risk management security issues prior to implementation, there is the additional potential risk of the FBLP computer operations staff's time being taken up with addressing production issues of the New ASP Black Lung System once it goes live, thereby preventing these high-risk security issues from being addressed."

The program strongly disagrees with this conclusion. First, as noted in the detailed responses above, DCMWC has already addressed each of these issues. Further, given the inherent strengths in system security cited in the report, it is highly unlikely that the "potential effects" speculated would manifest. Finally, DCMWC has conducted a complete risk assessment of the system and has submitted this assessment to the OCIO.

Medium-risk Management and Technical Security Control Issues

1. Security Awareness training did not include FBLP's policy against file and drive sharing via the network neighborhood.

Response: Security training has been conducted as part of the client server (C/S) training sessions and included a section devoted to this issue. All users have been made aware of this policy.

2. An excessive number of employees have access to the data center, but this may be appropriate due to the current development environment. However, once the application is in production, FBLP should re-evaluate personnel with access to the data center.

Response: The access list to the data center is reviewed on a routine basis. Personnel who no longer require access to the data center are removed from the access list.

3. The segregation of duties within the FBLP appears to be adequate. We are aware that due to system testing, access to particular application security screens is not finalized.

Response: A final check of the system user's access rights has been identified as a necessary activity prior to moving to production and has been included in the C/S PMP (item 64) for over a year. It has also been identified and included in the C/S "Implementation Plan."

4. Logical access controls over the Informix database appear appropriate, however, criteria has not been established to determine how RESOURCE and DBA level access will be granted once the ASP application is in production.

Response: In conjunction with system implementation, the criteria will be established for the logical access controls over the Informix database. Once this has been determined, the access will be evaluated for the Client Server list of appropriate individuals. This will be established and documented.

5. Access to the development instances of the ASP application has been appropriately granted during the development stage. While RESOURCE and DBA access is appropriate for the development stage, this can cause potential security weaknesses if not timely updated.

Response: In conjunction with system implementation, the RESOURCE and DBA access to the production instance will be reviewed and the criteria for the access will be documented. The access to production will then be evaluated and updated as necessary.

6. Full UNIX shell access has been granted under the current development environment. However, once the ASP goes into production, full shell access should be revoked for non-essential Testing, Software Development, Data Administration, DOL Project Team, and Network Services personnel.

Response: The listing of personnel with UNIX shell access is reviewed on a routine basis. Personnel who no longer require shell access are removed.

7. The configuration and change management procedures for the ASP software have not been finalized. The procedures are currently in draft form, and are based upon mainframe change management procedures found in the Hardware Configuration

Handbook (HCMH), Software Configuration Handbook (SCMH) and Technical Services Standards and Procedures (TSSP) documentation. The HCMH, SCMH and TSSP are scheduled for revision to incorporate the change from a mainframe to a client-server environment.

Response: The procedures will be updated and tracked in accordance with the CCB's ER process. Documentation is being updated. These procedures will mirror currently used mainframe configuration management processes. Please note that the Draft Report found that Informix database changes are properly documented and controlled and that system development life cycle procedures are adequate. Configuration and change management procedures are covered by these documents.

Medium-risk Management Security Control Issues Related to the Current FBLP Operating Environment

1. FBLP does not consistently utilize screen-saver technology on PCs connected to the LAN. The audit team was able to successfully gain access to seven unattended PCs and send e-mails from the users' mail accounts.

Response: DCMWC will evaluate this suggestion and will implement if feasible.

2. Visitors to the computer room are not required to sign a visitor's log.

Response: A visitors log has been implemented for the computer room.

3. The auditing functionality (e.g. – excessive log-on attempts) of the Novell network is disabled. The audit team recommends that certain auditing functionalities (sic) be reviewed to identify if they can be implemented without overly taxing system resources.

Response: Auditing of the NT networks is enabled. The audit list was reviewed and modifications were made to include failed occurrences. This will ensure that failed log-on attempts are captured. Auditing on the NetWare networks is not enabled at this time. The audit function of NetWare is extremely resource intensive and would have an impact on network performance. In regards to C/S, access to the NetWare Networks could only allow an intruder to access the application and does not provide access to the Sequent equipment. The application would be further controlled by the Security Master application code.

4. There are no procedures in place to periodically review the network neighborhood to ensure file and drive sharing does not occur.

Response: File and drive sharing is being addressed in the client-server security procedures. This document has been updated and is under internal review by federal and

contractor staff. Additionally, all staff received security training regarding the new system and were advised against this practice.

5. Network change control procedures (upgrades, software patches, configuration settings) are currently being revised to provide a uniform network change control process for the FBLP Novell and NT network environments.

Response: These procedures will be finalized in conjunction with implementation.

6. Procedures are currently being developed for periodic reviews of the FBLP network using the ISS Scanner. DCMWC plans on having ISS reports reviewed and submitted to DOL on a monthly basis.

Response: Procedures for these reviews will be finalized in conjunction with implementation. The FBLP Security Team reviews ISS reports on a monthly basis. The results are shared with the appropriate platform security personnel for risk assessment and mitigation. Documentation will be developed and/or finalized in conjunction with implementation.

7. Network change documentation does not include the person(s) responsible for network changes. Furthermore, management approval for each network change is not documented. The documentation does not include information indicating that the network changes were verified to ensure proper function of the network after the changes were made.

Response: The change control process utilized on the NT platform has been implemented on the NetWare platforms. This process includes the above mentioned features. The mirrored Microsoft NT process was deemed adequate on page 7 of the audit (Positive Security Control Audit Observations) where it states that "change to the Microsoft NT network environment appears to be adequately controlled and documented."

Medium-risk Management Security Control Issues Related to the DCMWC's District Offices

1. and 2. Issues identified at both the Johnstown and Greensburg District Offices:

- Wet-pipe fire sprinkler systems in/near the area of the network computer equipment.
- Updated DOL Security Awareness Training has not been conducted.

Response: DCWMC will meet with the landlord to determine whether changes to the sprinkler system can be made. Security training has been conducted as part of client server training.

3. The following issue was identified at the Johnstown Office only:

- The front-door cipher-locks are not changed on a regular basis or after an employee retires.

Response: DCMWC will revise procedures to resolve this problem.

4.,5. and 6. The following issues were identified at the Greensburg Office only:

- The Greensburg District Office Computer Equipment is located out in the open of the office, and its wires are exposed to potential unplugging and other unforeseen acts which may cause the District's connection to the Black Lung network inoperable.
- There were no visitor badges required.
- There appears to be a lack of enforcement of the sign-out log. Upon observation of the sign-out log, it appears that previous day visits were not required to sign out for the time they left the facility.

Response: DCMWC will review these items with the District Office.

Medium-risk Management Security Control Issues Related to the Current FBLP Network Environment

1. Password filter is not implemented on the FBLP network to enforce strong passwords (passwords containing at least 3 of the following: lowercase letters, uppercase letters, numbers, and special or non-numeric characters.)

Response: Required changes have been implemented. DCMWC has already instructed users to use "strong" passwords. Additionally, this topic was covered during the security portion of training on the new client server system. The DCMWC system support contractor (CSC) has incorporated the use of "L0phtCrack" on a monthly basis to ensure that "strong" passwords are utilized.

2. All passwords on 4 FBLP NT servers (including the Primary Domain Controller) and 2 FBLP Novell servers were successfully guessed by KPMG's password cracking utility.

Response: IDL and NCP Packet Signature Option Level 3 have been implemented. DCMWC has already instructed users to use "strong" passwords. Additionally, this topic was covered during the security portion of training on the new client server system. The DCMWC system support contractor (CSC) has incorporated the use of "L0phtCrack" on a monthly basis to ensure that "strong" passwords are utilized.

3. Password aging on Domain Administrator accounts has not implemented.

Response: Password aging has been implemented on the identified accounts.

4. The Web Server Folder Traversal Vulnerability exists on the FBLP's Microsoft Internet Information Server (IIS) web servers. This vulnerability involves a serious flaw in the IIS UNICODE translation and is extremely simple to exploit. It gives the attacker the ability to break out of the web server root directory, access and manipulate files in other locations, and execute arbitrary commands.

Response: DCMWC/CSC/Network Services has installed the patch as identified in the Microsoft security bulletin MS00-057 to eliminate this vulnerability.

5. The Remote database Services (RDS) Vulnerability exists on FBLP's web servers operating under Windows NT 4.0. This vulnerability allows an attacker on the Internet to run arbitrary commands with System level privileges or manipulate data on the FBLP web servers.

Response: DCMWC/CSC/Network Services removed three registry keys to eliminate this vulnerability per Microsoft security bulletin MS98-004.

DCMWC has addressed all but two of the issues noted above. With respect to these two issues, the program will evaluate the feasibility of using password-protected screen savers and will discuss dry-pipe options for the Johnstown and Greensburg offices with the landlords. As noted above, DCWMC has submitted a complete risk assessment to the OCIO.