

Office of Inspector General

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

Security Testing and Evaluations Pilot Audit of the Office of Workforce Security System

FINAL REPORT

This report was prepared by KPMG LLP, under contract to the Office of Inspector General, and, by acceptance, it becomes a report of the Office of Inspector General.

/s/

Assistant Inspector General for Audit

Report Number: 23-01-004-03-315
Date Issued: September 26, 2001

TABLE OF CONTENTS

I. Executive Summary	1
II. System Overview	2
III. Scope and Methodology	3
IV. Security Testing and Evaluation Summary Observations	4
A. Positive Observations on Security Controls	4
B. Observations on High-Risk Security Issues	5
C. Observations on Medium-Risk Security Issues	5
V. Security Testing and Evaluation Detailed Findings and Recommendations	7
A. General Security Issues	7
B. UNIX and Informix Issues	16
C. Network Security Penetration Testing Issues	25
Appendix A - Management Response to Draft Report	40
Appendix B – Acronyms.....	53

I. EXECUTIVE SUMMARY

PricewaterhouseCoopers LLP (PwC) under contract to the Office of Inspector General (OIG), performed a Security Testing and Evaluation (ST&E) pilot audit of the Office of Workforce Security (OWS) system. The purpose of the ST&E was to (1) test the effectiveness of the technical security features intended to protect sensitive information, and (2) determine the risk profile of the control environment. The results of our testing do not guarantee that future security compromises will not occur. It is the responsibility of DOL's management to ensure that adequate safeguards are implemented to reduce the probability of unauthorized access in the future. The information contained in our report can be used as input by DOL's system accrediting authority to incorporate the necessary security measures given the risk profile and sensitivity of the OWS system.

Security requirements that were tested were based on the Federal guidelines from Presidential Decision Directive 63 (PDD-63), OMB A-130, NIST 800-18, NIST 800-14, and NIST 800-12. Requirements stated in the DOL's Cyber Security Program Plan (CSPP), Computer System Security Plan (CSSP), and Computer Security Handbook (CSHB) were also used. In addition, the specific security requirements for the OWS System have also been taken from the Employment and Training Administration (ETA), which is responsible for the operations and maintenance of the system and the development of a security plan in accordance with NIST 800-18.

We tested 65 requirements across 9 security categories. Although we found a number of strong security controls, we identified 18 high and medium risk issues that need management attention. In summary we found:

- Overall improvements are needed in the Entitywide Security Program.
- The OWS systems are not certified in accordance with OMB A-130/FIPS 102.
- The security architecture is not fully defined and implemented.
- The security configurations standards are incomplete and/or inadequate.
- Security awareness training, including incident response is inadequate.

ETA has agreed with our observations and has taken steps to improve the security controls and reduce the security risk.

II. SYSTEM OVERVIEW

The ETA recently upgraded its Office of Workforce Security (OWS) system (formerly the Unemployment Insurance Service - UIS). The new OWS system has replaced the current system, which currently resides on two UNIX boxes. The OWS system has been identified by the U.S. Department of Labor (DOL) as a Presidential Decision Directive - 63 (PDD-63) system.

The OWS System is owned and used exclusively by the ETA. The OWS system is used to collect transmitted unemployment data from the states to a central database at the National Office. Additionally, the OWS system supports interactive access for users at the National Office and Regional Office locations. Support for interactive users includes electronic mail, office automation, database queries, and special modeling applications. Batch file transfers transmit unemployment data from the states to a central database at the National Office, electronic mail between various systems.

Wide area interactive access is achieved through frame relay capability at all regional locations. Batch file transfers between the National Office and the state sites occur primarily by asynchronous dial-up links and the UNIX-to-UNIX copy (UUCP) protocol. Each state has a Sun Ultra 10 minicomputer that is polled by two systems at the National Office. The main database server at the National Office polls each site during the evening. State sites are not allowed to dial into the National Office systems and are not considered part of the OWS UNIX system.

The National Office LAN is connected to the regions and the Internet through routers provided by OTIS. The OWS system is connected to the Internet through a network infrastructure operated by OTIS.

The OWS configuration consists of the following hardware and software:

Hardware Specifications

OWS System: Database - Sun E3500, Application - Sun 420R

Operating System Software/Version

UNIX: Sun Solaris 2.7 (SunOS 5.6)

Programming Language/Version

Informix 4GL, v7.3

Informix Online SQL Triggers, v7.2

Informix ESQL/C, v7.11

C, v4.2

Data Base Management Software/Version

Informix Online v7.2.UD2

III. SCOPE AND METHODOLOGY

A. Scope

Testing was performed to evaluate requirements for the following nine categories:

1. System Identification
2. Vulnerability Assessment
3. Technical Controls
4. Personnel Controls
5. Physical Controls
6. Maintenance Controls
7. Education and Awareness
8. Contingency Planning
9. Public Access Controls

The scope of this ST&E did not include the system interfaces with the states and did not include external network security penetration testing.

B. Methodology

Security requirements tested for the evaluation were based on Federal, DOL, and Agency requirements, as agreed to by Management, the OIG, and the Project Team.

Security requirements that were tested were based on the Federal guidelines from Presidential Decision Directive 63 (PDD-63), OMB A-130, NIST 800-18, NIST 800-14, and NIST 800-12. Requirements stated in the DOL's Cyber Security Program Plan (CSPP), Computer System Security Plan (CSSP), and Computer Security Handbook (CSHB) were also used. In addition, the specific security requirements for the OWS System have also been taken from the Employment and Training Administration, which is responsible for the operations and maintenance of the system and the development of a security plan in accordance NIST 800-18.

We identified any security requirements uniquely applicable to the OWS System. Additionally, we identified new and updated Federal regulations and DOL requirements pertaining to the system. Agency specific requirements for the system were obtained and included in the testing program. The agency reviewed the requirements being used for evaluation of the system and provided authorization that the requirements were valid and accurate.

IV. SECURITY TESTING AND EVALUATION SUMMARY OBSERVATIONS

We tested a total of 65 vulnerabilities across 9 testing categories. The following table highlights the tests by level of risk.

Vulnerability Matrix

Category	Number of Requirements Tested	Number of Vulnerabilities Tested by Level of Risk			
		High	Medium	Low	Total
System Identification	11	2	6	3	11
Vulnerability Assessment	3	0	3	0	3
Technical Controls	19	11	8	0	19
Personnel Controls	7	4	3	0	7
Physical Controls	5	4	1	0	5
Maintenance Controls	9	4	5	0	9
Education & Awareness	4	3	1	0	4
Contingency Planning	6	4	2	0	6
Public Access Controls	1	0	1	0	1
Total	65	32	30	3	65

A. Positive Observations on Security Controls

We identified positive security measures in place over the OWS System.

- There were no physical access control vulnerabilities identified.
- Backup policies and procedures are in place and followed accordingly.
- Physical Security controls within the ETA computer room located on the 6th floor of the DOL headquarters building have been established and are followed appropriately.
- The ETA has developed a System Development Life Cycle (SDLC) and has updated the document accordingly.
- A Warning banner is displayed at login for both the OWS application and database servers.
- ETA had restricted direct network access to the two primary OWS servers.
- ETA detected and responded to the activities of the penetration testing team.

B. Observations on High-Risk Security Issues

As a result of our testing, we identified the following 10 high-risk security control issues:

General Security Issues

- (1) ETA-OWS has not implemented a mandatory, security awareness training program, including incident response training, for all employees.
- (2) The ETA OWS system contingency plan has not been adequately tested.

UNIX and Informix Issues

- (3) Guest accounts with no password were found on OWS application server and weak passwords on user and application accounts were found on the OWS systems.
- (4) World-writeable files and directories were found on the OWS application and database servers.
- (5) No auditing was performed on the OWS production database.
- (6) Due to weak segregation controls, unauthorized users may gain access to OWS production because production, test, and development OWS databases reside on the same server.

Network Security Penetration Testing Issues

- (7) Windows NT password quality in the UIS-DIT domain was poor.
- (8) Two UNIX machines were not kept up-to-date with the latest security patches.
- (9) Trust relationships between UNIX machines permitted remote access without requiring passwords.
- (10) Configuration of NFS mounted directories allowed escalation of privileges.

C. Observations on Medium-Risk Security Issues

We identified the following eight medium-risk security control issues:

General Security Issues

- (1) The ETA OWS does not have documented Rules of Behavior to govern staff use of the computer system.
- (2) The OWS system has not been certified and accredited, per OMB A-130 or FIPS 102 standards.

UNIX and Informix Issues

- (3) Generic and test accounts exist on the OWS systems.

Network Security Penetration Testing Issues

- (4) User information was available on Windows NT servers without first logging in.
- (5) Excessive network services were accessible from within and outside the UIS subnet.
- (6) Accounts existed with the same username and password on UNIX as on Windows NT.
- (7) FTP software facilitated identification of valid UNIX usernames.
- (8) Excessive information was available, via DNS, providing complete lists of the registered machines names and IP addresses.

V. FINDINGS AND RECOMMENDATIONS

A. General Security Issues

Number of Observations: 4

Category VII
Requirement 3

Condition:

The ETA OWS has not adopted a formal security awareness training program. In addition, security awareness training is not a requirement for the ETA OWS staff. This information was not specifically addressed by the ETA OWS Security Plan.

Cause:

Although a security awareness program is currently in place and is held once a year, it is not mandatory for all ETA employees.

Criteria:

OMB A-130

"The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency."

"Each user should be versed in acceptable behavior -- the rules of the system -- before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system."

"Agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability."

NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, states that, "All applications and systems must be covered by system security plans if they are categorized as a *major application* or *general support system*."

Effect:

By not requiring employees to attend security and incidence response training sessions, ETA is exposed to the risk of their employees not being prepared to respond effectively to system security incidents.

Recommended Corrected Action:

We recommend that ETA OWS management implement a mandatory, biannual security awareness training session for its employees. In addition, ETA should record these large training sessions and offer it to those staff unable to attend the course in person.

Management Comments:

ETA's CIO & Security Officer (OTIS) responded to this finding in the remediation plan submitted to the Department on Aug 24, 2001 .

Auditor Response to Management Comments:

ETA OWS Management will need to implement its remediation plan with an established completion date in order to resolve this issue..

Category VIII
Requirement 2

Condition:

The ETA OWS has tested its Disaster Recovery and Contingency plan on a piecemeal basis. Portions of the contingency plan have been tested as minor failures occur; however, ETA OWS has yet to test the contingency plan in its entirety.

Cause:

The ETA does not have a policy (as part of the System Security Plan) stating that the Disaster Recover and Contingency plan must be tested.

Criteria:

OMB A-130, Appendix III

Section A, Requirements

Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

Section B, Descriptive Information

Contingency Planning. Normally the Federal mission supported by a major application is critically dependent on the application. Manual processing is generally NOT a viable backup option. Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

Effect:

The ETA OWS has no assurance that the plan they have developed will actually have the ability to effect the recovery of critical business operations in the event of a disaster.

Recommended Corrected Action:

We recommend that ETA test the OWS Disaster Recovery and Contingency Plan in its entirety. This testing should be done on an annual basis or whenever significant changes are made to the IT architecture plan or when key personnel changes. In addition, the Disaster Recovery and Contingency Plan should be updated to reflect such changes.

Management Comments:

OWS has requested funding to support this task in the FY 2002 budget. If the budget request is approved, OWS will address testing of the disaster recovery and contingency plan in FY2002.

Auditor Response to Management Comments:

Management needs to complete its testing of the Disaster Recovery and Contingency Plan in order to be compliant with OMB A-130 and PDD – 67.

<p>Category IV Requirement 1</p>	<p>Condition: The ETA OWS does not have documented Rules of Behavior to govern staff use of the computer system. This information was not specifically addressed by the ETA OWS Security Plan.</p> <p>Cause: The ETA does not have a policy (as part of the System Security Plan) stating that the Rules of Behavior must be documented and adhered to by all employees.</p> <p>Criteria: OMB A-130 "An important new requirement for security plans is the establishment of a set of rules of behavior for individual users of each general support system. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy, as described in 'An Introduction to Computer Security: The NIST Handbook' (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training. " "Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability." NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, states that, "All applications and systems must be covered by system security plans if they are categorized as a <i>major application</i> or <i>general support system</i>." Effect: Employees cannot be held accountable for their actions related to computer usage if there is no policy requiring the staff to review the Rules of Behavior document.</p> <p>Recommended Corrected Action: We recommend that ETA:</p> <ol style="list-style-type: none"> 1. Develop formal Rules of Behavior, addressing all appropriate OMB and NIST requirements, as well as any other ETA specific requirements. 2. Require all employees and contractors to review these Rules of Behavior and sign an agreement stating that they will act according to these Rules of Behavior prior to granting user access. 3. Conduct a yearly review of the Rules of Behavior ensuring that it reflects DOL ETA's current environment.
--------------------------------------	--

Management Comments:

OWS has referred this issue to ETA's CIO and Security Officer to develop a Rules of Behavior for the federal staff. ETA's Security Officer has addressed the issue in remediation plan submitted to DOL on Aug 24, 2001.

OWS will address this issue for the DDSS contractor staff in the next release of the OWS System Security Plan. OWS intends to have a implemented Rules of Behavior and enforcement procedure by December 31, 2001.

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition.

Category I
Requirement 6

Condition:

The OWS system has not been certified and accredited, per OMB A-130 standards. ETA conducted a self-review of the OWS system prior to the ST&E, yet was not effective in meeting a certification and accreditation process.

Cause:

ETA has not presented evidence or documentation to support adequate certification and accreditation procedures for the OWS system. ETA has stated that proper certification and accreditation will take place at the end of FY 2002.

Effect:

For a system currently in production, such as OWS, it is essential for the system to be certified and accredited in order for it to be a trusted system.

Criteria:

OMB A-130

"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 the Appendix."

NIST 800-12: An Introduction to Computer Security

A computer system should be accredited before the system becomes operational with periodic re-accreditation after major system changes or when significant time has elapsed. Even if a system was not initially accredited, the accreditation process can be initiated at any time.

Recommended Corrected Action:

We recommend that ETA obtain the required certification and accreditation for OWS.

Management Comments:

OWS-DDSS is currently reviewing the FIPS PUB 102 and OMB A-130 standards as suggested by the OIG. However, we have not received any formal guidelines at the departmental or agency level on the process. OWS will refer this issue to the ETA's CIO and Security Officer.

However, OWS has definitely made tangible progress in its security initiatives and have effectively reduced the scope of known vulnerabilities. OWS management is responsive to security issues and continues to make additional improvements to security of its systems.

	Auditor Response to Management Comments:
--	---

Management needs to continue its efforts to work with the Department on establishing and implementing a Certification and Accreditation process.

V. FINDINGS AND RECOMMENDATIONS (CONTINUED)

B. UNIX and Informix Issues

Number of Observations: 5

Category III
Requirement 9

Condition:

Testing revealed weak password configurations for OWS systems, specifically:

- Weak passwords for user accounts on the OWS system.
- Guest account with no password on the application server.
- Password aging and expiration for accounts are not set on the OWS system.

Cause:

ETA has not enforced the password requirements stated in the OWS security policy and Federal guidelines for user accounts on the OWS system.

Criteria:

NIST 800-18: Guide for Developing Security Plans for Information Technology Systems, addresses the following password requirements.

- Allowable character set
- Password length (minimum, maximum)
- Password aging time frames and enforcement approach
- Number of generations of expired passwords disallowed for use

Effect:

The ETA has no assurance that the OWS system is protected from unauthorized use or access when user accounts are protected with null or weak passwords.

Recommended Corrected Action:

We recommend that ETA OWS take the following corrective actions:

1. At a minimum, a process should be established to periodically run a password-cracking program to identify and change all easy-to-guess passwords. Security software should be used to enforce the use of strong passwords.
2. Passwords should immediately be assigned to accounts that currently have no passwords associated with them. If no user is associated with the account, the user ID should be locked or removed from the local password file.
3. Password aging and expiration should be set in accordance with OWS security policy or federal guidelines.

Management Comments:

OWS currently uses CRACK and plans to also provide automatic lockout of cracker passwords and an automatic generation of email to users with faulty passwords. OWS will also update the password policy to include requiring passwords to be 8

characters. Password aging and expiration will be set to 90 days on all UNIX servers. These items are scheduled to be completed by September 2001.

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been made.

Category III
Requirement 7

Condition:

The ETA OWS has not removed the permission for world-writable and setUID/setGID files and directories from the OWS system.

Cause:

The ETA OWS has not fully enforced its policy of least privilege in terms of access to files and programs on the OWS system.

Criteria:

NIST 800-6 Automated Tools for Testing Computer System Vulnerability

The discretionary access controls associated with a typical operating system provide some degree of potential security. For convenience, configuration files set system and user defaults for the file protection attributes. This frees users from specifying the protections assigned for every file created. However, the security achieved will be minimal if a user's default file protections are "read/write/execute by ANYONE." In each of these cases, little actual security is achieved. If a user makes these mistakes, the damage is confined to portions of the system that the user can access. If that user is the system administrator, the entire system is at risk.

NIST 800-13 Telecommunications Security Guidelines for Telecommunications Management Network, states "Data Confidentiality deals with protecting against the disclosure of information by ensuring that the data is limited to those authorized or by representing the data in such a way that its semantics remain accessible only to those who possess some critical information (e.g., a key for decrypting the enciphered data)." In addition, the guidelines states "The NE shall support mechanisms that ensure the confidentiality of sensitive information stored, processed and transmitted by the system."

Effect:

The ETA has no assurance in the integrity of the data and file system on the OWS system if users on the system can modify or delete their contents. Poorly designed setUID/setGID files could potentially be abused by malicious users, allowing them to execute a shell with privileged access. Once at the shell prompt, the user would retain the same access as the actual owner of the setUID/setGID files.

Recommended Corrected Action:

We recommend that ETA OWS ensure that:

1. All writable-by-other files be reviewed. Unless the writable-by-other permission is needed for the proper functioning of the system, the permission should be changed.
2. All setUID/setGID files be reviewed. If setuid/setgid is required, the program should be compiled and all access to the source code should be restricted. Otherwise, the setUID/setGID permissions should be removed.

Management Comments:

OWS has reviewed all files and changed permissions where appropriate. Only files which are required for proper functioning of the system remain unchanged.

In-house generated application files are reviewed by Management and OPS security staff before production implementation and source code is secured by Configuration Management.

OWS has indicated that the above corrective actions have already been taken.

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been made.

<p>Category III Requirement 10</p>	<p>Condition: The ETA OWS has not enabled auditing on the OWS database to monitor for changes made to critical tables and granting of access on the OWS database.</p> <p>Cause: The ETA OWS has no requirements to monitor access and changes made to the OWS production database.</p> <p>Criteria: NIST 800-13: Telecommunications Security Guidelines for Telecommunications Management Network, Section 4.6, page 20, states that "the NE shall generate logs that contain information about security relevant events. Items selected for recording shall be defined and selected by the security administrator. The logs shall enable security administrators to investigate losses and improper actions on the part of users, legitimate and otherwise, and to seek legal remedies."</p> <p>Effect: The ETA has no means, via an audit trail, to ensure the accountability of changes made to the OWS production database.</p> <p>Recommended Corrected Action: We recommend that ETA implement auditing on the OWS database to include, at the minimum, the following events:</p> <ul style="list-style-type: none"> • Create Role (CRRL) • Set Role (STRL) • Set Session Authorization (STSA) • Set Object Mode (STOM) • Open Database (OPDB) • Grant/Revoke Database Access (GRDB), (RVDB) • Grant/Revoke Table Access (GRTB), (RVTB) • Grant/Revoke Role (GRRL), (RVRL) • Grant/Revoke Fragment Access (GRFR), (RVFR) <p>Management Comments: OWS indicates they are reviewing the ability to enable auditing on this system and will have completed this review by September 30, 2001.</p> <p>Auditor Response to Management Comments: We support management's corrective plan to study the possibility of enabling the auditing attribute.</p>
--	---

<p>Category VI Requirement 2</p>	<p>Condition: The development, test and production instances of the database for the UI application are all running on the same server. The Informix database will allow users with access to the operating system (UNIX) to have access to all three instances.</p> <p>Cause: The authentication process allowing access to the Informix database is performed at the operating system level (UNIX) and not at the database level.</p> <p>Criteria: NIST 800-18: Guide for Developing Security Plans for Information Technology Systems stresses that there be a distinction between live data and test data.</p> <p>Effect: Given the nature of weaknesses noted at the operating system level, this creates a vulnerability that allows an unauthorized user to connect to any of the three instances (development, test and productions databases) from the operating system creating a risk of denial of service.</p> <p>Recommended Corrected Action: We recommend that ETA OWS segregate the production environment in a manner that would prevent an unauthorized user from disrupting the production environment. In addition, a policy regarding this segregation approach should be created and incorporated as part of the system development life cycle methodology.</p> <p>Management Comments: Though all users of the OWS system have some level of access to the different instances of the databases, restrictions are in place to prevent unauthorized users from accessing sensitive UI data.</p> <p>Due to cost implications, OWS is unable to accommodate this recommendation for segregation of the production database.</p> <p>Auditor Response to Management Comments: Management needs to reconsider this condition and implement alternative corrective actions to monitor unauthorized access to the sensitive UI data. A risk still exists for unauthorized access and denial of service to the production environment.</p>
---	--

Category III
Requirement 6

Condition:

Weaknesses were identified in user accounts:

- There are 150 out of 183 users on the application server (UI) and 19 users on the database server (Hera) that have access to a UNIX command shell.
- Generic and test accounts are found on the application and database servers.
- There are 177 out of 183 users on the application server and 340 users out of 351 users on the database server that have not logged in for more than 60 days.

Cause:

There were three causes. First, the ETA OWS has no requirements that would disallow access by users to a UNIX command shell. Second, at the time of our testing, ETA had not fully completed the migration of the OWS application to the new application server. Our testing revealed that test and generic accounts still exist on the server. On the database server, test and generic accounts also exist because the test and development instances of the OWS database reside on the same server as the production instance. Third, the ETA OWS does not enforce its policy of reviewing user accounts on a monthly basis to determine if any users need to be removed from a group or a system.

Criteria:

NISTIR 5153, Minimum Security Requirements for Multi-User Operating Systems, Section 3.3.1 #5, states "The system shall automatically disable userIDs after a period of time during which the userID has not been used. The time period shall be customer-specifiable, with a default of sixty days."

NIST 800-18: Guide for Developing Security Plans for Information Technology Systems, Section 6.MA.2/6.GSS.2, page 40 and 61, states that an organization should "indicate how often access control lists are reviewed to identify and remove users who have left the organization ore whose duties no longer require access to the application."

Effect:

User accounts exist that provide access authorizations exceeding normally expected needs. ETA does not have assurance that users are granted access privileges that are necessary to perform their duties.

Recommended Corrected Action:

We recommend that ETA OWS:

1. Users should be restricted from having command-line access to the OWS system.
2. Generic accounts should be removed from the local password file. Users who accessed the system via these generic accounts should be given unique individual accounts.
3. Accounts that have not been accessed for an extended period of time should be disabled.

Management Comments:

OWS is reviewing user access to the command line based on the application requirements and will attempt to restrict some end users. The review is scheduled to be completed by September 30, 2001.

Test accounts not in use have been disabled. Also, OWS has set shell accounts to “nologin” for database server”. OWS indicates that this corrective action has already been taken.

In regards to recommendation #3 OWS states that the snapshot used by the penetration testing team was prior to the production setup. No users are currently allowed to login into the database server except for support purposes. Other accounts with no login privileges are setup on the database server to provide the necessary connectivity for end user tools such as SPSS etc. Manual review of user accounts are done every 30 days and password expiration on servers have been set for 90 days.

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been made.

V. FINDINGS AND RECOMMENDATIONS (CONTINUED)

C. Network Security Penetration Testing Issues

Number of Observations: 9

<p>Category III Requirement 4</p>	<p>Condition: Poor Windows NT password quality in the UIS-DIT domain.</p> <p>Cause: Windows NT, as installed by ETA, does not enforce a strong password policy. The testing team correctly guessed the password of an administrator account. With this level of access the testing team could control all machines within the domain. The testing team used this access to download the password information for all users in the domain, and then used the L0phtcrack tool to crack over 95% of the passwords within 12 hours.</p> <p>Criteria: NIST 800-12: An Introduction to Computer Security, states that "if users are not allowed to generate their own passwords, they cannot pick easy-to-guess passwords." These include generic vendor-provided words. FIPS 112 states, "Passwords that are created by the Security Officer for new users of the system during initial system access shall be selected at random from all acceptable passwords." Also, "users that create or select their own personal password shall be instructed to use a password selected from all acceptable passwords at random, if possible, or to select one that is not related to their own personal identity, history, or environment." NISTIR 5153, Minimum Security Requirements for Multi-user Operating Systems, states "The system shall store passwords in a one-way encrypted form.</p> <ul style="list-style-type: none"> • The system shall require privilege to access encrypted passwords. • Unencrypted passwords shall be inaccessible to all users." <p>Effect: Unauthorized access to user and administrative accounts can be obtained compromising the system availability, confidentiality and integrity.</p> <p>Recommended Corrective Action: We recommend that ETA OWS:</p> <ul style="list-style-type: none"> • Set and enforce a strong password policy – both in writing and by computer configuration. • Enable passfilt.dll and then require all users to change passwords. • Periodically run L0phtcrack or a similar tool on all accounts to identify and correct weak passwords.
---------------------------------------	---

Management Comments:

OWS indicated that it will:

- Upgrade Password policy: must change password every 90 days, password must be 10 characters in length with alphanumeric & special characters, account locked out after 3 failed attempts. (OWS indicates that this corrective action has been taken.)
- Create separate admin accounts for support staff requiring administrator privileges. (OWS indicates that this corrective action has been taken.)
- Apply NT workstation security patches (On-Going Task)
- Encrypt SAM database and improve NT password policy. (OWS indicates that this corrective action has been taken.)
- Procurement of LOphtrcrack in process. (Implementation TBD).

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. In addition, management should continue to consider enabling passfilt.dll. Auditor will need to re-test the configuration settings to ensure that the above changes have been implemented.

Category III
Requirement 4

Condition:

Two UNIX servers were susceptible to known security vulnerabilities – specifically the *dtappgather* vulnerability and the *ufsrestore* vulnerability. The penetration testing team exploited these known vulnerabilities to gain root access on two UNIX servers.

Cause:

Applicable patches or upgrades were not installed as well as the lack of a plan to address known security vulnerabilities.

Criteria:

NIST SP 800-6 Automated Tools for Testing Computer Systems Vulnerability, Section 1

To ensure that an acceptable level of security is achieved, the administrator should utilize automated tools to regularly perform system vulnerability tests. The tests examine a system for vulnerabilities that can result from improper use of controls or mismanagement. Examples of such vulnerabilities include:

- easily guessed passwords;
- improperly protected system files;
- opportunities for planting Trojan horses; and
- failure to install security-relevant bug fixes.

Effect:

Unauthorized access to user and administrative accounts can be obtained compromising the system availability, confidentiality and integrity.

Recommended Corrective Action:

We recommend that ETA OWS install applicable patches or upgrade to a newer version of the operating system that resolves these security vulnerabilities, in accordance with a documented software maintenance plan.

Management Comments:

All servers are to be upgraded to recommendation patch levels. This is an on-going process.

OWS will improve security on the servers by configuring software that provides added security (YASSP). OWS has indicated that this correction action has been taken the following servers: Athena, Apollo, Eris, Hermes, Artemis, and Hestia. Correction action will be taken on UI, Hera and Zeus by September 30, 2001.

	<p>Auditor Response to Management Comments:</p>
--	--

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been implemented.

Category III
Requirement 4

Condition:

Trust relationships between UNIX machines facilitated remote access without requiring passwords. The penetration testing team exploited trust relationships to transfer user and root access from compromised UNIX servers to those that trusted them.

Cause:

The trust relationships were established using the r-services configured with .rhosts and /etc/hosts.equiv.

Criteria:

OMB Circular A-130 requires agencies to implement the practice of least privilege whereby user access is restricted to the minimum necessary to perform his or her job; and enforce a separation of duties so that steps in a critical function are divided among different individuals. It also emphasizes the importance of management controls – such as individual accountability requirements, separation of duties enforced by access controls, and limitations on the processing privileges of individuals – to prevent and detect inappropriate or unauthorized activities.

Effect:

Unauthorized access to other systems via the compromised systems using the trust relationship.

Recommended Corrective Action:

We recommend that ETA OWS:

- Eliminate or minimize trust relationships.
- Eliminate the r-services and associated files. Replace with ssh or similar for remote access.

Management Comments:

OWS will:

- Tighten up trust relationships to support Informix & GUI applications. (OWS indicates that this corrective action has been taken.)
- Remove .rhosts file and turn off rsh, rlogin, rexec, rcp. (OWS indicates that this corrective action has been taken.)
- Install Secure Shell (SSH) client and server software for DDSS National Office Users. (OWS indicates that this corrective action has been taken on OWS Clients/Servers. Awaiting schedule from ETA's CIO and Security Officer for SSH client implementation ETA Wide).

	<p>Auditor Response to Management Comments:</p>
--	--

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been implemented.

Category III
Requirement 4

Condition:

NFS mounted directories allowed escalation of privileges. Using a server where the network security penetration testing team already had root access, the team copied a command shell to a directory which was being exported via NFS, and made it setuid root. Then, from a target machine that had mounted the exported directory, the team ran the command shell to gain root access.

Cause:

The default configuration of NFS mounted directories support the setuid feature of UNIX, which permits users to run programs as if they were another user.

Criteria:

OMB Circular A-130 requires agencies to implement the practice of least privilege whereby user access is restricted to the minimum necessary to perform his or her job; and enforce a separation of duties so that steps in a critical function are divided among different individuals. It also emphasizes the importance of management controls – such as individual accountability requirements, separation of duties enforced by access controls, and limitations on the processing privileges of individuals – to prevent and detect inappropriate or unauthorized activities.

Effect:

Users can gain a level of access that is inconsistent with their job responsibilities. In addition, unauthorized users can exploit this vulnerability to compromise the system security.

Recommended Corrective Action:

We recommend that ETA OWS:

- Review the arrangement of NFS mounted directories.
- For all NFS mounted directories, use the nosuid option.

Management Comments:

OWS reviewed NFS/UFS mounts and set read only on mounts wherever possible. OWS does not allow suid on NFS/UFS wherever possible. (OWS indicates that these corrective actions has been taken.)

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been implemented.

<p>Category III Requirement 4</p>	<p>Condition: Accounts existed with the same username and password on UNIX as on Windows NT. The penetration testing team used compromised usernames and passwords gained from Windows NT to access UNIX servers.</p> <p>Cause: Lack of password policy and enforcement.</p> <p>Criteria: FIPS 112 states, "Passwords that are created by the Security Officer for new users of the system during initial system access shall be selected at random from all acceptable passwords." Also, "users that create or select their own personal password shall be instructed to use a password selected from all acceptable passwords at random, if possible, or to select one that is not related to their own personal identity, history, or environment."</p> <p>Effect: Unauthorized users that gain entry to one server can use the information to compromise other servers on the network.</p> <p>Recommended Corrective Action: We recommend that ETA OWS use different usernames and passwords on different systems. This should be accomplished through policy, accounts management procedures, awareness measures, and manual enforcement.</p> <p>Management Comments: OWS will establish different passwords policy for UNIX and NT accounts. (OWS indicates that this corrective action has been taken.). OWS will also conduct further review of the password quality. (In progress).</p> <p>Auditor Response to Management Comments: Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been made.</p>
---------------------------------------	--

<p>Category III Requirement 4</p>	<p>Condition: Ftp software identified which usernames were valid and which were not by giving different error messages during authentication. The penetration testing team used this flaw to screen for valid usernames, based on the compromised Windows NT accounts, and found a valid username and password on a UNIX machine within 85 minutes.</p> <p>Cause: Flaw in the design of the versions of ftp software used.</p> <p>Criteria: NIST 800-12: An Introduction to Computer Security, states that "if users are not allowed to generate their own passwords, they cannot pick easy-to-guess passwords." These include generic vendor-provided words.</p> <p>Effect: This setting greatly increases the efficiency of a password guessing attack by helping the attacker guess passwords only for valid usernames.</p> <p>Recommended Corrective Action: We recommend that ETA OWS switch to a version of ftp that gives the same error message, regardless of whether or not the username is valid.</p> <p>Management Comments: OWS will replace FTP with secure FTP (SFTP) by September 30, 2001.</p> <p>Auditor Response to Management Comments: Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that a secure FTP (SFTP) version has been installed.</p>
---------------------------------------	---

<p>Category III Requirement 4</p>	<p>Condition: Excessive information was available via DNS. The penetration testing team quickly obtained complete lists of the registered machines names and IP addresses and clues about the purposes of those machines. This helped the team to focus their attack more efficiently.</p> <p>Cause: DNS servers were configured to allow unrestricted zone transfers.</p> <p>Criteria: OMB Circular A-130 requires agencies to implement the practice of least privilege whereby user access is restricted to the minimum necessary to perform his or her job; and enforce a separation of duties so that steps in a critical function are divided among different individuals. It also emphasizes the importance of management controls – such as individual accountability requirements, separation of duties enforced by access controls, and limitations on the processing privileges of individuals – to prevent and detect inappropriate or unauthorized activities.</p> <p>Effect: This setting provides additional information to an unauthorized user, making it easier to compromise system security.</p> <p>Recommended Corrective Action: We recommend that ETA OWS set the DNS servers to allow zone transfers only to other authorized DNS servers.</p> <p>Management Comments: OWS will upgrade to higher versions of BIND on Apollo and Zeus to allow only trusted hosts zone transfer. (Implementation scheduled by October 31, 2001). OWS will also install local perimeter protection host for UNIX servers. (Implementation scheduled by October 31, 2001 or sixty days after the hardware receipt.)</p> <p>Auditor Response to Management Comments: Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been made.</p>
---------------------------------------	---

Category III
Requirement 4

Condition:

User information was available on Windows NT servers without first authenticating. The network security penetration testing team obtained a list of all users and groups within the UIS-DIT domain without providing a valid username and password. This dramatically reduced the amount of time required to compromise the domain, since password guessing was focused on known accounts with administrator level access. The team correctly guessed the password of an administrator account 57 minutes after obtaining the lists.

Cause:

The default configuration of Windows NT makes this information available.

Criteria:

NIST SP 800-6 Automated Tools for Testing Computer Systems Vulnerability,

The basic rules for the content and protection of User Files are derived by considering the testing objectives. User files must not permit the installation of Trojan horse programs. Users must restrict access to objects they create according to the organization's security policy. The following rules support these goals:

- Protect personal start-up files from modification by others. (These files are ideal candidates for planting Trojan horses since they are ALWAYS executed.)
- Do not specify personal or shared directories before system-provided directories in executable search paths. (This invites the installation of Trojan horses.)
- Default protections assigned at file creation should meet system standards.
- Limit write access in a user's personal file space (by appropriate protection of user directories).

Effect:

Unauthorized access to user and administrative accounts can be obtained compromising the system availability, confidentiality and integrity.

Recommended Corrective Action:

We recommend that ETA OWS:

- Set the RestrictAnonymous registry value on Windows NT/2000 machines.
- Allow Authenticated Users, instead of Everyone, to access Windows NT/2000 machines from the network.
- Establish network filters that block all unnecessary network services from outsiders, particularly TCP/UDP ports 135, 137, 139.

Management Comments:

OWS indicates that they have already implemented the first two of the “Recommended Corrective Actions”.

In order to establish network filters block all unnecessary network services from outsiders, OWS intends to:

- Ensure that the OTIS firewall is address all unnecessary network traffic.
- Encrypt SAM database. (OWS indicates that this corrective action has been taken.)
- Disable test account ‘qa_test’. (OWS indicates that this corrective action has been taken.)
- Turn on “failed login” audit logging with alert. (OWS indicates that this corrective action has been taken.)
- Secured system using Microsoft’s NT security checklist. (OWS indicates that this corrective action has been taken.)
- Update NT Server security patches. (On-Going task).
- Disable null connection to Mordred and Orion. (OWS indicates that this corrective action has been taken.)

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition. Auditor will need to re-test the configuration settings to ensure that the above changes have been made.

Category III
Requirement 4

Condition:

Excessive network services were accessible from within and outside the OWS subnet. Specifically: telnet, Microsoft NetBIOS/RPC, r-services and ftp were significant during penetration testing. The penetration testing team used these network services to compromise several UIS systems.

Cause:

Insufficient network access controls over vulnerable network services.

Criteria:

OMB Circular A-130 requires agencies to implement the practice of least privilege whereby user access is restricted to the minimum necessary to perform his or her job; and enforce a separation of duties so that steps in a critical function are divided among different individuals. It also emphasizes the importance of management controls – such as individual accountability requirements, separation of duties enforced by access controls, and limitations on the processing privileges of individuals – to prevent and detect inappropriate or unauthorized activities.

Effect:

Users can gain a level of access that is inconsistent with their job responsibilities. In addition, unauthorized users can exploit this vulnerability to compromise the system security.

Recommended Corrective Action:

We recommend that ETA OWS disable or replace vulnerable network services, where possible. Use protocol filtering to permit only authorized machines to use network services. This can be done at a router, switch or firewall on the network. Use TCP Wrappers on UNIX servers, or the TCP/IP filtering feature on Windows NT servers.

Management Comments:

OWS has and will take the following actions:

- Reviewed and updated /etc/services and /etc/inetd.conf to restrict/remove services. (OWS indicates that this corrective action has been taken.)
- Install Secure shell (SSH) client and server software for DDSS support staff. (SSH implementation complete on OWS Client/Servers. Awaiting schedule from ETA's CIO and Security Officer for SSH client implementation ETA wide.)
- Install local perimeter protection host for UNIX servers. (Implementation scheduled by October 31, 2001 or sixty days after hardware receipt).
- TCP wrappers are already implemented on all OWS UNIX systems and have been in use since 1995.

- | | |
|--|--|
| | <ul style="list-style-type: none">▪ Review of the TCP/IP filtering feature on Windows NT servers are in progress. (Implementation scheduled by October 31, 2001 or sixty days after hardware receipt). |
|--|--|

Auditor Response to Management Comments:

Management actions proposed to address this condition appear reasonable and appropriate and should, if properly implemented, sufficiently address the condition.

Auditor will need to re-test the configuration settings to ensure that the above changes have been made.

OWS Security Upgrade Plan
 OWS Response to OIG’s Draft Report

Finding/Condition	Recommended Corrective Action	Response	Time Frame
<p>THE ETA OWS has not adopted a formal security awareness training program. In addition, security awareness training is not a requirement for the ETA OWS staff. This information was not specifically addressed by the ETA OWS Security Plan.</p>	<p>ETA OWS management should implement a mandatory, biannual security awareness training session for its employees. In addition, ETA should record these large training sessions and offer it to those staff unable to attend the course in person.</p>	<p>ETA’s CIO & Security Officer (OTIS) responded to this finding in the remediation plan submitted to the Department on Aug 24, 2001 .</p>	<p>ETA’s Security Officer has addressed the issue in remediation plan submitted to DOL on Aug 24, 2001.</p>
<p>The ETA OWS has tested its Disaster Recovery and Contingency plan on a piecemeal basis. Portions of the contingency plan have been tested as minor failures occur; however, ETA OWS has yet to test the contingency plan in its entirety.</p>	<p>DOL ETA test the OWS Disaster Recovery and Contingency plan in its entirety. The testing should be done on an annual basis or whenever significant changes are made to the IT architecture plan or when key personnel changes. In addition, the Disaster Recovery and Contingency Plan should be updated to reflect such changes.</p>	<p>OWS has requested funding to support this task in the FY 2002 budget. If the budget request is approved, OWS will address testing of the disaster recovery and contingency plan in FY2002.</p>	<p>FY2002</p>

<p>THE ETA OWS does not have documented Rules of Behavior to govern staff use of the computer system. This information was not specifically addressed by the ETA OWS Security Plan.</p>	<p>1. Develop formal rules of behavior, addressing all appropriate OMB and NIST requirements, as well as any other ETA specific requirements.</p> <p>2. Require all employees and contractors to review these Rules of Behavior and sign an agreement stating that they will act according to these Rules of Behavior to grant user access.</p> <p>3. Conduct a yearly review of the Rules of Behavior ensuring that it reflects DOL ETA's current environment.</p>	<ul style="list-style-type: none"> • OWS will review the documented Rules of Behavior for DDSS contractor staff in the security plan as per the guidelines and will make revisions as required. • For an overall Rules of Behavior for OWS Federal staff within ETA, OWS referred the issue to ETA's CIO and Security Officer. • OWS will address this issue for DDSS contractor staff. • For the rules of behavior review and signoff by OWS Federal staff within ETA, OWS referred the issue to ETA's CIO and Security Officer. • Will incorporate this recommendation in the next update of the OWS security plan. • For review cycle of rules at the ETA level, OWS will refer to issue to ETA Security Officer. 	<p>Next update of the OWS security plan based on the timeline set by the CIO.</p> <p>ETA's Security Officer has addressed the issue in remediation plan submitted to DOL on Aug 24, 2001.</p> <p>Implementation by Dec 31, 2001.</p> <p>ETA's Security Officer has addressed this issue in the remediation plan submitted to DOL on Aug 24, 2001.</p> <p>Next update of the OWS security plan based on the timeline set by the CIO.</p> <p>ETA's Security Officer has addressed this issue in remediation plan submitted to DOL on Aug 24, 2001.</p>
---	---	--	--

<p>The OWS system has not been certified and accredited per OMB A-130 standards. ETA conducted a self-review of the OWS system prior to the ST&E, yet was not effective in meeting a certification and accreditation process.</p>	<p>ETA -OWS should obtain the required certification and accreditation for OWS.</p>	<p>OWS-DDSS is currently reviewing the FIPS PUB 102 and OMB A-130 standards as suggested by the OIG. However, we have not received any formal guidelines at the departmental or agency level on the process. OWS will refer this issue to the ETA's CIO and Security Officer.</p> <p>However, OWS has definitely made tangible progress in its security initiatives and have effectively reduced the scope of known vulnerabilities. OWS management is responsive to security issues and continues to make additional improvements to security of its systems.</p>	<p>OWS will address this issue to the ETA's CIO and Security Officer.</p>
---	---	--	---

<p>ETA OWS needs to enforce OWS security policy and federal guidelines on password management. Testing revealed:</p> <ul style="list-style-type: none"> ▪ Weak passwords for user accounts on the OWS system. ▪ Guest account with no password on the application server. ▪ Password aging and expiration for accounts are not set on the OWS system. 	<p>1. At a minimum, a process could be established to periodically run a password-cracking program to identify and change all easy-to-guess passwords. Security software could be used to enforce the use of strong passwords.</p> <p>2. Passwords should immediately be assigned to accounts that currently have no passwords associated with them. If no user is associated with the account, the user id should be locked or removed from the local password file.</p> <p>3. Password aging and expiration should be set in accordance with OWS security policy or federal guidelines.</p>	<p>OWS already uses and executes CRACK on a regular basis to identify easy-to-guess passwords. A manual process to alert users to change passwords is also in place. Additional upgrades for this utility are planned which include -</p> <ul style="list-style-type: none"> (1) provide automatic lockout of cracked passwords (2) Automatic generation of email to users with faulty passwords <p>Improve UNIX password quality filters.</p> <p>Update password policy to 8 characters</p> <p>Need additional clarification from OIG regarding guest account. We have no accounts setup with login access which do not have a password entry.</p> <p>Password aging has been set for 90 days expiry on all UNIX servers.</p> <p>Password aging and expiration for all UNIX servers has been set for 90 days.</p>	<p>Implementation scheduled by 9/14/2001</p> <p>Implementation scheduled by 9/14/2001</p> <p>Implementation Complete</p> <p>Implementation Complete</p> <p>Request for clarification from OIG.</p> <p>Implementation Complete</p>
--	---	--	---

<p>ETA/OWS has not removed the permission for world-writable and setUID/setGID files and directories from the OWS system.</p>	<p>1. All writeable-by-other files be reviewed. Unless the writeable-by-other permission is needed for the proper functioning of the system, the permission should be changed.</p> <p>2. All setUID/setgid files be reviewed. If setuid/setgid is required, the program should be compiled and all access to the source code should be restricted. Otherwise, the setUID/setGID permissions should be removed.</p>	<p>OWS has reviewed all files and changed permissions where appropriate. Only files which are required for proper functioning of the system remain unchanged.</p> <p>In-house generated application files are reviewed by Management and OPS security staff before production implementation and source code is secured by Configuration Management.</p>	<p>Implementation Complete.</p> <p>Implementation Complete.</p>
---	--	--	---

<p>ETA/OWS has not enabled auditing on the OWS database to monitor for changes made to critical tables and granting of access on the OWS database.</p>	<p>Implement auditing on the OWS database to include at the minimum the following events:</p> <ul style="list-style-type: none"> ▪ Create Role (CRRL) ▪ Set Role (STRL) ▪ Set Session Authorization (STSA) ▪ Set Object Mode (STOM) ▪ Open Database (OPDB) ▪ Grant/Revoke Database Access (GRDB), (RVDB) ▪ Grant/Revoke Table Access ▪ Grant /Revoke Role ▪ Grant /Revoke Fragment Access 	<p>Under Review by OWS</p>	<p>Sept 30, 2001</p>
<p>The development, test and production instances of the database for the UI application are all running on the same server. The Informix database will allow users with access to the operating system (UNIX) to have access to all three instances.</p>	<p>ETA should segregate the production environment in a manner that would prevent an unauthorized user from disrupting the production environment. In addition, a policy regarding this segregation approach should be created and incorporated as part of the system development life cycle methodology.</p>	<p>Though all users of the OWS system have some level of access to the different instances of the databases, restrictions are in place to prevent unauthorized users from accessing sensitive UI data.</p> <p>Due to cost implications, OWS is unable to accommodate this recommendation for segregation of the production database.</p>	

<p>Management of user accounts on the OWS system needs to be improved.</p> <ul style="list-style-type: none"> ▪ 150 out of 183 users on the application server (UI) and 19 users on the database server (Hera) have access to a UNIX command shell. ▪ Generic and test accounts are found on the application and database servers. ▪ 177 out of 183 users on the application server and 340 users out of 351 users on the database server have not logged in for more than 60 days. 	<ol style="list-style-type: none"> 1. Users should be restricted from having command-line access to the OWS system. 2. Generic accounts should be removed from the local password file. Users who accessed the system via generic accounts should be given unique individual accounts. 3. Any accounts that have not been accessed for an extended period of time should be disabled. 	<p>We are reviewing the user access based on the application requirements and will attempt to restrict some end users.</p> <p>Test accounts not in use have been disabled until required. Also set shell accounts to 'nologin' for database server.</p> <p>The snapshot used by the penetration testing team was prior to the production setup. No users are currently allowed to login into the database server except for support purposes. Other accounts with no login privileges are setup on the database server to provide the necessary connectivity for end user tools such as SPSS etc. Manual review of user accounts are done every 30 days and password expiration on servers have been set for 90 days.</p>	<p>Sept 30, 2001</p> <p>Implementation Complete.</p> <p>Implementation Complete</p>
--	--	---	---

<p>Poor Windows NT Password quality in the UIS-DIT domain was observed.</p>	<ul style="list-style-type: none"> ▪ Set and enforce strong password policy - both in writing and by computer configuration. ▪ Enable passfilt.dll and then require all users to change passwords. ▪ Periodically run LOphthcrack or similar tool on all accounts to identify and correct weak passwords. 	<p>Upgrade Password policy : must change password every 90 days, password must be 10 characters in length with alphanumeric & special characters, account locked out after 3 failed attempts.</p> <p>Create separate admin accounts for support staff requiring administrator privileges.</p> <p>Apply NT workstation security patches</p> <p>Encrypted SAM database and improved NT password policy.</p> <p>Procurement of LOphthcrack in process.</p>	<p>Implementation Complete</p> <p>Implementation Complete</p> <p>Implementation Complete (Ongoing task)</p> <p>Implementation Complete</p> <p>Implementation Complete</p> <p>Implementation TBD</p>
---	--	---	--

<p>Two UNIX servers were susceptible to known security vulnerabilities - specifically the dtappgather vulnerability and the ufsrestore vulnerability. The penetration testing team exploited these known vulnerabilities to gain root access to two UNIX servers.</p>	<p>Install applicable patches or upgrade to a newer version of the operating system that resolves these security vulnerabilities, in accordance with documented software maintenance plan.</p>	<p>All servers upgraded to recommended patch levels.</p> <p>Improved security on the servers by configuring software which provides added security (YASSP).</p> <ul style="list-style-type: none"> ▪ UI ▪ Hera ▪ Athena ▪ Apollo ▪ Zeus ▪ Eris ▪ Hermes ▪ Artemis ▪ Hestia 	<p>Implementation Complete (Ongoing task).</p> <p>by Sep 30,2001 by Sep 30,2001 Implementation complete Implementation complete by Sep 30, 2001 Implementation complete Implementation complete Implementation complete Implementation complete</p>
---	--	---	---

<p>Trust relationships between UNIX machines facilitated remote access without requiring passwords. The penetration testing team exploited trust relationships to transfer user and root access from compromised UNIX servers to those that trusted them.</p>	<ul style="list-style-type: none"> ▪ Eliminate or minimize trust relationships. ▪ Eliminate the r-services and associated files. ▪ Replace with ssh or similar for remote access. 	<p>Tighten up trust relationships to support Informix & GUI applications</p> <p>Removal of .rhosts files and turn off rsh, rlogin, rexec, rcp.</p> <p>Install Secure shell (SSH) client and server software for DDSS National Office users.</p>	<p>Implementation complete</p> <p>Implementation Complete</p> <p>SSH implementation on OWS Clients/Servers Complete. Awaiting schedule from ETA's CIO and Security Officer for SSH client implementation ETA wide.</p>
<p>Configuration of NFS mounted directories allowed escalation of privileges. Using a server where the network security penetration testing team already had root access, the team copied a command shell to a directory which was being exported via NFS, and made it setuid root. Then, from a target machine that had mounted the exported directory, the team ran the command shell to gain root access.</p>	<ul style="list-style-type: none"> ▪ Review the arrangement of NFS mounted directories. ▪ For NFS mounted directories, use the nosuid option. 	<p>OWS reviewed NFS/UFS mounts and set read only on mounts wherever possible.</p> <p>No suid on NFS/UFS mounts wherever possible.</p>	<p>Implementation complete</p> <p>Implementation complete</p>

<p>Accounts existed with the same username and password on UNIX as on NT. The penetration testing team used compromised usernames and passwords gained from Windows NT to access UNIX servers</p>	<p>Use different usernames and passwords on different systems</p>	<p>Established different passwords policy for UNIX and NT accounts.</p> <p>Further review of the password quality is in progress.</p>	<p>Implementation Complete</p> <p>Ongoing</p>
<p>FTP software identified which usernames were valid and which were not by giving different error messages during authentication. The penetration testing team used this flaw to screen for valid usernames, based on the compromised Windows NT accounts, and found a valid username and password on a UNIX server within 85 minutes.</p>	<p>Switch to a version of FTP that gives the same error message regardless of whether or not the username is valid.</p>	<p>Replace FTP with a secure FTP (SFTP).</p>	<p>Sept 30, 2001</p>
<p>Excessive information was available via DNS. The penetration testing team quickly obtained complete lists of the registered machines names and IP addresses and clues about the purposes of those machines. This helped the team to focus their attack more efficiently.</p>	<p>Set the DNS servers to allow zone transfers only to other authorized DNS servers.</p>	<p>Upgrade to higher versions of BIND on Apollo & Zeus to allow only trusted hosts zone transfer.</p> <p>Install local perimeter protection host for UNIX servers</p>	<p>Implementation scheduled by Oct 31, 2001</p> <p>Implementation scheduled by Oct 31, 2001 (or sixty days after hardware receipt)</p>

<p>User information was available on Windows NT servers without first authenticating. The network security penetration testing team obtained a list of all users and groups within the UIS-DIT domain without providing a valid username and password. This dramatically reduced the amount of time required to compromise the domain, since password guessing was focused on known accounts with administrator level access. The team correctly guessed the password of an administrator account 57 minutes after obtaining the lists.</p>	<ul style="list-style-type: none"> ▪ Set the RestrictAnonymous registry value on Windows NT/2000 machines ▪ Allow Authenticated users, instead of everyone, to access Windows NT/2000 machines from the network. ▪ Establish network filters that block all unnecessary network services from outsiders, particularly TCP/UDP ports 135,137,139. 	<p>OTIS firewall is expected to address all unnecessary network traffic from outsiders.</p> <p>Encrypt SAM (Security Account Manager storing user/password entries) database</p> <p>Disable test account (qa_test)</p> <p>Turn on 'failed login' audit logging with alert.</p> <p>Secured system using Microsoft's NT security checklist.</p> <p>Update NT server security patches.</p> <p>Disable null connection to Mordred and Orion</p>	<p>Implementation Complete</p> <p>Implementation Complete</p> <p>Verification with ETA's CIO and Security Officer (OTIS) pending</p> <p>Implementation Complete</p> <p>Implementation Complete</p> <p>Implementation Complete</p> <p>Implementation Complete</p> <p>Implementation Complete (Ongoing task)</p> <p>Implementation Complete</p>
---	---	---	---

<p>Excessive network services were accessible from within and outside the UIS subnet. Specifically: telnet, Microsoft NetBIOS/RPC, r-services and ftp were significant during penetration testing. The penetration testing team used these network services to compromise several UIS systems.</p>	<p>Disable or replace vulnerable network services where possible. Use protocol filtering to permit only authorized machines to use network services. This can be done at a router, switch or firewall on the network. Use TCP Wrappers on UNIX servers, or the TCP/IP filtering feature on Windows NT servers.</p>	<p>Reviewed and updated /etc/services and /etc/inetd.conf to restrict/remove services.</p> <p>Install Secure shell (SSH) client and server software for DDSS support staff.</p> <p>Install local perimeter protection host for UNIX servers</p> <p>TCP wrappers are already implemented on all OWS UNIX systems and have been in use since 1995.</p> <p>Review of the TCP/IP filtering feature on Windows NT servers are in progress.</p>	<p>Implementation Complete</p> <p>SSH implementation on OWS Clients/Servers Complete. Awaiting schedule from ETA's CIO and Security Officer for SSH client implementation ETA wide.</p> <p>Implementation scheduled by Oct 31, 2001 (or sixty days after hardware receipt)</p> <p>Implementation scheduled by Oct 31, 2001 (or sixty days after hardware receipt)</p>
--	--	---	---

S:\OIS\DDSS\SECURITY\Security Response Plan.ver1.3.wpd

ACRONYMS

CSHB	Computer Security Handbook
CSSP	Computer System Security Plan
CSPP	Cyber Security Program Plan
DOL	Department of Labor
ETA	Employment and Training Administration
FTP	File Transfer Protocol
LAN	Local Area Network
OIG	Office of Inspector General
OMB	Office of Management and Budget
OWS	Office of Workforce Security
PDD	Presidential Decision Directive
PwC	PricewaterhouseCoopers
ST&E	Security Testing and Evaluation
SDLC	System Development Life Cycle
TFARS	Tentative Findings and Results
UIS	Unemployment Insurance Service
UUCP	UNIX to UNIX copy protocol