Computer Security Controls Should Be Strengthened in the Houston District

July 2000

Reference Number: 2000-20-106

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

July 18, 2000

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Scott E. Wilson

FROM: Scott E. Wilson
Associate Inspector General for Audit (Information Systems Programs)

SUBJECT: Final Audit Report - Computer Security Controls Should Be Strengthened in the Houston District

This report presents the results of our review of computer security controls in the Houston District. In summary, we found that steps should be taken to strengthen the Houston District's systems to guard against and detect inappropriate accesses. We made recommendations to improve security controls in the areas of user account management, security surveillance, and physical security.

Management's response was due on July 10, 2000. As of July 18, 2000, management has not responded to the draft report.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-8510 if you have questions, or your staff may call Steve Mullins, Director (Systems Security), at (925) 210-7024.

Table of Contents

Executive Summary

Advances in information technology have caused the daily activities of the Internal Revenue Service (IRS) to become increasingly automated and inter-linked. These advances, while improving efficiency, have also increased the risk that hackers or dishonest employees could misuse taxpayer data. Recent events have demonstrated the risk of hackers gaining inappropriate access to other government agencies and private businesses. Malicious acts by employees present an even greater risk since they already have access to data via networks. The Houston District has over 800 employees connected to its Windows NT[1] local area network (LAN), approximately 150 of whom have access to taxpayer information through the Examination Returns Control System (ERCS).[2]

The overall objective of this review was to determine whether the Houston District has effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss. We reviewed controls over the District's LAN with emphasis on the ERCS to help define our scope and demonstrate the impact of security weaknesses. This review was part of a series of reviews initiated to assess the overall effectiveness of security controls over the IRS' information systems.

Results

The District has various computer security controls in place which reduce the risk, to some degree, of unauthorized access and destruction of data. For example, logical access controls, such as user identification and passwords, were properly set up at the minicomputer and LAN level, and logical access to sensitive system areas, such as the ERCS, was correctly limited. In addition, physical access to the working area and computer facilities was properly restricted. However, additional steps in the following areas can further strengthen the computer security program.

Strengthening User Account Management, Security Surveillance, and Physical Security Controls Can Achieve a Higher Level of Security

Following prescribed controls can reduce information systems security weaknesses in the following three areas:

[1] Windows NT is a Microsoft network operating system with enhanced security capabilities.
[2] ERCS is an automated inventory management system for controlling tax returns under audit and technical time charges.

- **User Account Management**: The level of system access was inappropriate for several users. Special capabilities to research the ERCS had been granted to 41 Examination employees, 30 of whom, in our opinion, had no need for it. Those employees had the capability to run production reports by group and by employee. The use of such reports for evaluative purposes is specifically prohibited by law and IRS policy. We were unable to determine if evaluative production reports were actually generated because controls were insufficient to detect this activity.

  Acting managers were given ERCS approval authority for periods longer than needed, increasing the risk that they could approve inappropriate actions on their own work. In addition, three users who had access to the LAN, but not to the ERCS, were not removed promptly from the LAN after they had left the IRS. We did not identify any inappropriate activity by these three users.
- **Security Surveillance**: Activity logs (audit trails) were deactivated on some minicomputers. When audit trails were run on other minicomputers and the LAN, there was no indication they had been reviewed. Essentially, the District did not use audit trails to detect improper activity on its computer systems.
- **Physical Security**: There was no library log to record the removal and return of computer tapes. Also, access to the library was not sufficiently restricted.

Summary of Recommendations

The Chief Information Officer and IRS executives responsible for systems in the Houston District need to take steps to address the specific weaknesses identified in this report. Actions management should take include: allowing only appropriate system permissions and monitoring the use of the permissions; ensuring system access is promptly removed for departing employees; training and monitoring responsible employees on performing audit trail reviews; and reinforcing backup tape inventory controls.

Management's response was due on July 10, 2000. As of July 18, 2000, management has not responded to the draft report.

Objective and Scope

Our objective was to determine whether the Houston District has effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss.

The overall objective of this review was to determine whether the Internal Revenue Service's (IRS) Houston District has effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss.

We visited two sites in the District (the headquarters and the Alliance building post-of-duty) during January 2000. We selected the Examination Returns Control System (ERCS)[1] to help define our scope and demonstrate the impact of security weaknesses. In the sites we visited, we reviewed user account management, security surveillance, physical security, and logical access controls for the Windows NT[2] local area network (LAN), minicomputers, and the ERCS. We performed these reviews in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization meet its mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

[1] The ERCS is an automated inventory management system for controlling tax returns under audit and technical time charges.
[2] Windows NT is a Microsoft network operating system with enhanced security capabilities.

The IRS, along with other high-profile government agencies and corporations, is at risk of outsiders' efforts to break into its LANs. Advances in information technology have caused the daily activities of the IRS to become increasingly automated and inter-linked. These advances, while improving efficiency, have also increased the risk that hackers or dishonest employees could misuse taxpayer data. Malicious acts by employees present an even greater risk since they already have access to networks, in addition to being physically located where the hardware is housed.

Physical and logical access controls, restricting users' privileges, and monitoring system activity are all tools to help ensure adequate security.

Achieving adequate security depends on properly applying several types of controls. These can be categorized into the following four groups:

- User Account Management – The processes to establish and delete computer system users as well as to grant access privileges specific to an individual's official duties.
- System Security Surveillance – The ability to log and monitor computer system activities for indications of security violations as well as to timely respond to such incidents.
- Physical Security – The ability to limit physical access to computer system components (workstations, servers, and networks) to only those who are authorized and to provide a suitable physical surrounding which protects computer system components from man-made and natural hazards.
- System Logical Access – The ability to restrict access to computing resources within the computer system to those having a need-to-know.

The Congress recognized the significance of maintaining adequate information system security in the IRS Restructuring and Reform Act of 1998 (RRA 98).[3] This law directs the Treasury Inspector General for Tax

[3] Pub. L. No. 105-206, 112 Stat. 685.

Administration (TIGTA) to report to the Congress an assessment of the adequacy and security of the IRS' information technology. This report is part of TIGTA's effort to provide that assessment.

Results

Although various controls in place reduced risks to some degree, additional steps can strengthen the computer security program.

The District has various computer security controls in place which reduce the risk, to some degree, of unauthorized access and destruction of data. For example, logical access controls, such as user identification and passwords, were properly set up at the minicomputer and LAN level, and logical access to sensitive system areas, such as the ERCS, was correctly limited. Physical access to the working area and computer facilities was properly restricted.

Additional steps can strengthen the computer security program. Over 800 employees have access to the District's LAN, approximately 150 of whom have access to taxpayer information through the ERCS. A lack of control over such sensitive data increases the risk that it can be improperly disclosed or misused, possibly to commit fraud or other crimes.

Strengthening User Account Management, Security Surveillance, and Physical Security Controls Can Achieve a Higher Level of Security

Weaknesses in user account management allowed several users higher levels of system access than was appropriate. In addition, security surveillance was not sufficient to detect improper computer activity, and inadequate inventory controls created vulnerabilities in physical security over backup tapes.

User Account Management

User account controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computing resources.

Managers granted unneeded access privileges to users and did not remove users from systems when they no longer required access. These conditions occurred because managers were not thoroughly familiar with user account management requirements. In addition, security reviews conducted by users' managers did not detect the excessive permissions. In some instances, we were unable to determine whether inappropriate usage occurred and, in other instances, we determined it did not occur, as explained further in the following sections.

To reduce the risk of fraud and taxpayer privacy violations, access to IRS systems and applications must be limited to those users who require access to perform their jobs. Employees must be removed timely from systems or applications which they do not need to access. In addition, user activity should be periodically monitored to ensure access to taxpayer data is proper and for official purposes only.

An excessive number of employees had ERCS database research capability.

IQ software gives users access to personal information for thousands of taxpayers on the ERCS, and the capability to create production reports. Seventy-three percent of users having this access did not need it, in our opinion.

Intelligent Query (IQ) is software that allows users to research the ERCS database and create customized reports. It can be used when standard ERCS reports do not provide the required data. IQ gives users the capability to create production reports by employee and group. The use of such reports for evaluative purposes is specifically prohibited by law and IRS policy. It also gives users access to tax information for thousands of taxpayers. To prevent unauthorized reports and to protect the personal information of thousands of taxpayers from browsing or unauthorized disclosure, managers must restrict IQ capability to as few employees as possible.

Forty-one ERCS users in the Houston District Examination Division have IQ in their user profile. We believe that 30 of the 41 users (73 percent) have no need for this application. This occurred because users retained this capability after they transferred to other positions or simply no longer needed it. Furthermore, there is no policy defining who should have access to IQ and how this access should be controlled and monitored. Managers did not adequately assess the employees' need for IQ when conducting reviews of employees' system accesses and privileges.

Additionally, the use of IQ is not adequately controlled or monitored. To ensure that research of taxpayer data in the ERCS database is for authorized purposes only, all requests for IQ reports should be approved and documented, including a description of the purpose and intended use of the data. There are no procedures requiring requests for IQ reports to be approved and in writing.

It is especially critical to limit and monitor the use of IQ because managers have no audit trails[4] to detect unauthorized use. The ERCS application does not capture IQ activity and the UNIX[5] system captures only system-level activity, such as when a user enters or exits IQ. Because of the insufficient audit trail information, we were unable to detect whether evaluative production reports or any other inappropriate usage of IQ occurred.

Temporary ERCS permissions for acting managers were not adequately controlled.

Examination group managers may temporarily grant employees acting for them the authority to approve actions, or update (close) cases. The manager can grant this approval through the ERCS menu, or in the manager's absence, another manager can submit a written request to the ERCS coordinator who will grant the approval permission. This authority should be delegated for the shortest possible period of time and revoked upon the manager's return.

[4] Audit trails are a control for detecting improper activity on computer systems. Generally, they should show who took the action, what they did, where they did it, and when.

[5] UNIX is the operating system running on the District's minicomputers.

Managers did not limit agent's acting authority for the shortest possible period of time needed to accomplish the tasks.

On one day during our review, January 5, 2000, six revenue agents had temporary approval permission. Three of the six were given the permission for a 90-day period, longer than the duration of the managers' absences. In one of these three instances, the group manager did not provide or request the permission; instead, the revenue agent made the request to the ERCS coordinator on his own behalf. In addition to the six agents above, two other revenue agents were granted permanent approval authority by the ERCS coordinator instead of temporary permission, and another two agents were granted temporary authority to take actions such as closing cases and updating case statutes.

Currently, the ERCS cannot systemically prevent acting managers from taking actions on their own cases. Inappropriate actions taken with temporary update or approval authority could lead to violations of taxpayer rights and embezzlement.

Managers did not ensure that approval authority was granted for the shortest period of time. Managers did not periodically review audit trail records to identify employees using temporary approval or update permission to take actions on their own cases.

Users were not timely removed from the LAN.

Three of 43 Examination Division employees who separated from the Division during 1999 continued to have access to the LAN up to 4 months after their separation dates. In one case, the manager was aware that a form was required to remove the employee from the LAN, but had not timely completed it. In the other two instances, managers were not aware that the form was needed. None of the three were ERCS users or had access to any other applications containing taxpayer or sensitive data, and none accessed the LAN after separating. These employees also had Integrated Data Retrieval System access that was appropriately cancelled prior to their separation dates.

Security Surveillance

Audit trails are the primary control for detecting improper activity on computer systems. Generally, they should show who took the action, what they did, where they did it, and when. Although there is no audit trail for IQ, audit trails were available to detect activity on the LAN, on the minicomputers, and on the ERCS application running on the minicomputers. However, we noted weaknesses relating to all three audit trails.

The Internal Revenue Manual and other guidelines require that system administrators generate and distribute audit trails to appropriate managers for review. Functional security coordinators should review audit trails to ensure system integrity and to report anomalies. Security administrators should also review audit logs at least weekly and provide reports of security problems to the system administrators, the Information Systems Chief, and functional managers. User managers should ensure that audit trails are appropriately reviewed.

On the LAN, the operating system generates a security log, which contains audit trail information. There was no documentation that any reviews of this information had taken place.

In some cases, audit trails were not run, and when they were run, there was no evidence that they were reviewed.

The audit trails were deactivated for the three minicomputers on which the ERCS resides. This situation occurred because the system lacks the hardware resources to run the audit trail and the ERCS application at the same time. The audit trail slowed the system response time to a level that did not adequately service the users.

For the ERCS application running on the minicomputers, there were no scheduled reviews of the audit trail information, and any reviews that may have been done were not documented. The functional coordinator could have run audit trail reports that show requested actions, record updates, permissions, approvals, employee records and researched records.

Audit trails were run for the remaining minicomputers. However, there were no regularly scheduled reviews or monitoring of system administrator activities. Additionally, there was no documentation of any reviews that may have taken place. Officials advised that these reports are difficult to understand, and neither the vendor nor National Office staff have been able to assist them.

Although there are clear requirements for gathering and reviewing audit trail information, the requirements are often not specific regarding how to conduct the reviews and how they should be documented. In the absence of these guidelines, District management did not devise interim or local procedures to ensure the reviews were completed and adequately documented.

The ability to log and monitor computer system activities is important because it provides a means to detect improper activities that could occur if other system controls are circumvented. When audit trails are not running or properly monitored, the ability to identify offenders and pinpoint weaknesses to prevent future occurrences is lost.

Physical Security

Physical security is the most fundamental form of information systems control and is important because it is the first barrier in preventing unauthorized access and loss of taxpayer information. Physical security controls are implemented to protect sensitive areas housing information systems equipment or data. Sensitive areas requiring physical controls include computer rooms, communication wire closets, and areas housing essential support equipment, such as power control panels, air conditioning units, communication equipment, and magnetic media storage.

Controls over backup tapes need strengthening.

Information systems capture electronic data on magnetically charged disks and tapes, commonly referred to as magnetic media. Effective media management ensures accountability and accessibility of disks and tapes to operate the IRS' information systems. Without proper media protection, critical taxpayer data could be lost or compromised.

There is no library log for recording the removal and return of tapes to the library. However, library personnel are required to document the removal of magnetic media. In addition, admittance to the tape library should be restricted to only those with a need to access the tapes to prevent unauthorized access to taxpayer information. Although the room is secured with a cipher lock, the E-mail administrator, who has no need to access the tapes, works in the room.

Managers did not identify and ensure that weaknesses in tape library controls were addressed and corrected.

When records are not kept or are not current and access is not restricted, the risk of unauthorized disclosure of taxpayer information and not detecting missing tapes increases.

Recommendations

The Chief Information Officer and IRS executives responsible for systems in the Houston District need to take steps to address the specific weaknesses identified in this report.

Management's response was due on July 10, 2000. As of July 18, 2000, management has not responded to the draft report.

<u>User Account Management</u>

1. Review all users having IQ capability and restrict its use to those needing such access. Ensure that annual reviews of user account permissions include IQ

usage. Develop a policy defining who should have IQ access and how to control and monitor it. Develop procedures that require all non-routine IQ requests to be approved and documented, including the purpose intended and use of the data. Explore the feasibility of obtaining from the ERCS application those reports that are commonly requested through IQ to limit the number of users who need access to IQ.

2. Ensure that temporary approval permissions granted to acting managers are given for the exact periods needed. Periodically run the ERCS report of approval permissions, to be reviewed by management. Ensure managers review audit trails to detect acting managers updating or approving their own cases.

3. Remind managers of requirements for and instructions on removing access privileges for departing employees.

Security Surveillance

4. Reinforce requirements to perform audit trail reviews on the minicomputers, the LAN and the ERCS. Provide training on how to perform reviews, including what to review and when, how to document reviews, and how to handle potential problems discovered. Provide guidance on analyzing audit trail output for minicomputer audit trails so they are easier to review.

5. Explore solutions to the hardware resource problem of running the ERCS minicomputer audit trail, including moving the ERCS to a different platform, or possibly running audit trails on a sampling basis if possible.

Physical Security

6. Ensure a log is kept of backup tapes removed from and returned to the library.

7. Restrict access to backup tapes by relocating the E-mail administrator or the tapes.

Conclusion

Strengthening computer security controls could potentially reduce manipulation, destruction, theft, or improper use or disclosure of sensitive data.

Like other IRS offices, the Houston District's systems contain large amounts of sensitive information, and can be accessed by a large number of employees. Strengthening computer security controls can help ensure that access to the sensitive information is restricted to only those having a legitimate business need to use the information.

Implementation of our recommendations could reduce: 1) opportunities to improperly manipulate or destroy data; 2) opportunities for theft; and 3) the risk of improper use or disclosure of sensitive taxpayer data.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service's (IRS) Houston District has effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss. The following four control areas each contain an overall objective, sub-objectives, and tests for the particular area.

USER ACCOUNT MANAGEMENT

The overall objective of this control area was to determine if management has implemented sufficient user account management controls to ensure that access to taxpayer data on the Local Area Network (LAN) is limited to authorized individuals on a need-to-know basis.

Sub-objective I: Determined if management has implemented procedures in line with the security policy of providing access based on the individual's demonstrated need to view, add, change or delete data.

A. Interviewed the Houston District Chief, Examination Division, the official responsible for the Examination Returns Control System (ERCS).

   1. Identified the policies and guidelines used in the District to ensure access to the system is limited based on the policy of least privilege.
   2. Identified the Division Chief's specific responsibilities for ensuring ERCS accesses and privileges are limited to a need-to-know basis.

B. Interviewed the ERCS functional coordinator, the Examination Division functional security officer, the UNIX[1] system administrator, and the LAN system administrator to obtain an understanding of the controls over the configuration of user profiles. Determined their specific responsibilities for ensuring access to the system is limited based on the policy of least privilege. Identified the procedures used to limit user access privileges to only that which is needed to perform official duties.

Sub-objective II: Determined if management has established procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of ERCS and LAN user accounts.

A. Interviewed the ERCS functional coordinator, the Examination Division functional security officer, the UNIX system administrator, the LAN system administrator, and

[1] UNIX is the operating system running on the District's minicomputers.

user managers to identify and document the procedures in place relating to requesting, establishing, issuing, suspending, and closing ERCS and LAN user accounts.

B. Obtained a master list of ERCS users from the system administrator. Selected a judgmental sample of 20 of the 142 ERCS user accounts from the master list for review to ensure access rights were documented, authorized, and reviewed.

   1. For the sample of ERCS users, verified the existence of an Automated Information Systems (AIS) User Registration/Change Request (Form 5081) to support the authorization of each account and the approval of all access rights and privileges.
   2. Reviewed user profiles for the sample of ERCS users to ensure duties were properly separated to minimize the possibility of fraud, waste, or abuse and to ensure that access rights and privileges assigned to each user were commensurate with the users' job responsibilities.

C. Determined if any Houston District Examination or Information Systems (IS) personnel continued to have ERCS or LAN access after separating from the IRS. Compared a list of Examination and IS employees who separated between January 1, 1999, and January 1, 2000, to the lists of current ERCS and LAN users. Identified:

   1. The length of time after separation that employees continued to have access to IRS systems.
   2. All LAN applications for which separated employees continued to have access, such as the ERCS, the Travel Reimbursement Accounting System, the Integrated Data Retrieval System, e-mail, etc.

D. Determined if ad-hoc queries can be made to research the ERCS database. Identified:

   1. All users with the research capability.
   2. Procedures for controlling the use of the research capability, such as requirements that queries be documented to show authorization, approval, and purpose.
   3. Procedures for monitoring the use of the research capability to ensure that all research performed was authorized and appropriate.

Sub-objective III: Determined if management has a control process in place to periodically review and confirm access rights.

A. Interviewed the Houston District Chief, Examination Division, to determine if formal procedures exist to ensure that ERCS user access rights are appropriately reviewed and modified to ensure that access rights remain commensurate with user job responsibilities.

1. Identified those responsible for conducting periodic reviews.
2. Determined how the Division Chief ensures that the periodic reviews are conducted.

B. Interviewed branch chiefs and group/section managers regarding responsibilities for conducting the periodic reviews.

1. Determined the procedures used to conduct the reviews.
2. Obtained documentation of reviews performed and evaluated the quality of the reviews to ensure that they are accomplishing the intended objective.

C. Determined if user managers annually certify that system access for each employee has been reviewed and is appropriate.

SECURITY SURVEILLANCE

The overall objective of this control area was to determine whether controls are effective to ensure that all activity involving access to and modifications of sensitive or critical files is logged, effectively reviewed, and responded to if incidents occur.

Sub-objective I: Determined if controls are effective over audit trails to ensure that all activity involving access to and modifications of sensitive or critical files is logged.

A. Evaluated the adequacy of the audit trail by determining whether the required information (log-ons, dates, times, places, applications and files used) is being recorded.

B. Attempted to gain access to the system using a variety of unauthorized logon IDs and passwords. Verified that the attempted log-ons are properly recorded on the audit trail.

C. Reviewed guidelines to identify audit trail policies and procedures, including reporting security violations.

D. Determined if the audit trail is protected from unauthorized modification by interviewing the system administrator and functional coordinator to identify who has access to the audit trails and what level of permission is granted. Determined what criteria the security administrator uses to turn on the audit log, whether they back up the audit trail, and how long it is retained.

E. Determined if data security personnel periodically review security configuration settings to ensure that system auditing settings are configured to provide sufficient audit trails.

Sub-objective II: Determined if controls over audit trails ensure that they are effectively reviewed and access is limited to a need-to-know.

A. Determined whether audit trails were being run and reviewed at the UNIX, LAN, and ERCS internal levels. If they were not being reviewed, determined the reason. Determined whether any security violation reports were issued, reported to management and investigated.

B. Determined the extent that IS system administrators, programmers, security analysts, functional coordinators and managers have access to the audit trails, if any guidelines have been developed for reviewing audit trails, if security logs are required to be reviewed on a regular basis, and if they have received training to review audit trails.

Sub-objective III: Determined if controls ensure prompt and appropriate responses to security incidents.

A. Evaluated the effectiveness of the procedures for recognizing and handling computer security incidents. Determined whether the procedures identify roles and responsibilities, include criteria for documenting, determining the seriousness, reporting, investigating, and imposing disciplinary action, and provide the ability to respond quickly and effectively.

B. Determined what instruction, direction and training the Security Specialist received for reporting security incidents.

PHYSICAL SECURITY AND ENVIRONMENTAL CONTROLS

The objective of this control area was to evaluate the effectiveness of physical and environmental security controls over the LANs and selected sensitive and mission-critical applications for physically restricting access to computer hardware and adequately safeguarding taxpayer data.

Sub-objective I: Determined whether local policies and procedures on physical security are sufficient to limit access to LAN system servers and workstations and to safeguard EDP equipment from theft or loss.

Identified the security controls in place regarding restricting entrance into workspaces and the computer room. Identified how maintenance/cleaning personnel are allowed into the computer room.

Sub-objective II: Determined whether entrances to computer facilities and functional users' work spaces are properly secured and protected to ensure only authorized personnel are allowed to enter.

A. Identified locations for all workstations, obtained building layouts and conducted walk-throughs of computer rooms and some work spaces in the Alliance and headquarters buildings to identify all computer hardware related to the application being reviewed. Determined if physical entrances to spaces are restricted to authorized personnel.

B. Determined if the District's computer room maintains a low profile and physical identification is limited. Determined if the computer room's entrances and construction meet standards and specifications. Determined whether the location prohibits direct, unrestricted accesses through the outside or a public hallway. Determined whether a computer room entrance log is used regularly and properly controlled.

Sub-objective III: Determined whether security controls over telecommunication points of entry for the applications and its workstations are adequate to provide a trusted path for sensitive data flow.

A. Obtained physical layout documentation and observed during walk-throughs whether there were any undocumented access points to the LAN.

B. Reviewed LAN documentation and toured the facility to locate where the LAN connections terminate to physical communications lines at the facility. Evaluated the level of security over these access points.

C. Observed entrances to telephone equipment rooms to determine whether they were unlabeled and properly secured. Obtained a map of connections in the telecommunications closet. Reviewed connections for proper labeling and connection per the map.

Sub-objective IV: Evaluated the adequacy of the fire protection system related to LAN/ WAN systems within the computer room.

A. Observed the computer room to determine whether it has automatic fire detection and extinguishing systems and if they are tested periodically by the manufacturer or service representative to ensure the systems are working as intended.

B. Determined if the fire detection system is protected by a backup power supply to ensure continuous operation.

Sub-objective V: Determined whether the environmental equipment is adequate to protect computer hardware from damage.

A. Determined if the ventilation and air conditioning are adequate to maintain appropriate temperature levels specified by the manufacturer.

B. Determined if thermometers and humidity indicators are routinely monitored.

C. Determined if physical and/or software controls are used to ensure that the hardware automatically shuts down if unacceptable computer room temperatures are reached.

D. Determined if an independent air conditioning system with backup power was installed.

Sub-objective VI: Determined whether the back-up policy and procedures are adequate to ensure continuity of service in the event of a system/application disruption of operation.

A. Interviewed appropriate IS personnel and obtained the details of the back-up procedure for the ERCS application and its data.

B. Determined if the back-up process is periodically tested to ensure that it performs as intended and whether the back-up tapes are periodically reviewed to ensure that the data are accurate and complete.

C. Conducted a walk-through of the off-site location for back-up tapes to evaluate the security level of the site. Ensured access is restricted to authorized personnel, a back-up log is maintained, and the site is not identified as a tape library.

D. Conducted a reconciliation of the back-up tape inventory for the ERCS application to ensure inventory accurately reflects the back-up inventory listing.

E. Discussed the procedure for ensuring the back-up process is working properly.

F. Determined the procedure for loading data from the back-up tapes and whether this procedure has been tested and works as intended.

IDENTIFICATION, AUTHENTICATION AND ACCESS CONTROLS

The overall objective of this control area was to evaluate whether logical security controls were effectively installed to protect the integrity and confidentiality of the information processed, transmitted and stored.

Sub-objective I: Evaluated whether logical controls were adequately implemented to identify and authenticate users of the LAN operating system:

A. Reviewed security plans, security policies and procedures for the LAN and selected system/applications to determine requirements for granting access to computer resources. Interviewed managers of security/system administrators to determine their procedures for monitoring LAN/application activities. Evaluated whether oversight of administrator activities adequately ensures that they have access to only the resources needed to do their job.

B. Interviewed security/system administrators to identify authentication software in use, obtain password policies, and determine procedures for generating and communicating LAN/application passwords to users.

C. Determined if unique user IDs and passwords are issued and if any group/generic user IDs and passwords exist. Reviewed accounts that did not have an associated password.

D. Determined if any security software is used to proactively screen passwords. Identified any automated tools used to restrict system access and to monitor the security and activity of the LAN/application.

E. Reviewed steps taken to monitor the system and to ensure that policies and procedures are being followed.

F. Determined if the duties of system administration and security monitoring are separated to deter and detect unauthorized access and changes to the system.

G. Evaluated whether password generation/assignment procedures prevent inadvertent disclosure of assigned passwords and whether the established password life is adequate, given the sensitivity of the information and the amount of risk associated should the system be compromised. Compared password policies to minimum Federal Information Processing Standards.

H. Interviewed users and observed their work area and logon process to determine if unique user IDs and passwords were issued, any group/generic user IDs and passwords exist, the user changed the password when initially logging on, the system prevents plain text display of the password when entered, and passwords are disclosed on any medium at the user's workstation.

I. Conducted an "after hours" security check, inspecting the users' work areas for passwords posted at the workstation and computers where the user did not sign-off or lock the terminal.

J. Reviewed operating system and user account security file and password parameters to determine if the system is set to enforce passwords meeting minimum standards and lock or disable user access when standards are not met. Ensured access to the password file was restricted to a limited number of people.

K. Determined whether encryption is used to protect passwords from disclosure and unauthorized modification. Determined if the system is set to erase the plain text memory of the password immediately after encryption, if the encrypted password is stored in a shadow file instead, and if there is a key that can be used to decrypt the passwords and whether the key is stored outside the system.

Sub-objective II: Evaluated the adequacy of logical controls to prevent unauthorized access to and modification of system software.

A. Determined if controls were properly implemented to restrict access and prevent unauthorized changes to the LAN operating system and the selected security software settings.

B. Determined if the security and access control features that came with the operating system were enabled and configured in accordance with the access authorizations established by the information resource owners.

C. Reviewed security system parameters to ensure that security profile or table settings are protected from unauthorized changes either by encryption or by limiting the paths to them and by restricting access to authorized personnel in the security function. Reviewed security profile override capabilities to ensure that they are restricted to a few trusted individuals.

D. Reviewed security software access audit trail reports and related access rules and authorizations to ensure that individual security file accesses match the level and type authorized.

E. Determined if controls were properly implemented to restrict access and prevent unauthorized changes to other sensitive or critical files and libraries. Observed non-administrator system users demonstrate whether they can gain access to these files and libraries and noted the type of access that they have.

<u>Sub-objective III</u>: Evaluated the adequacy of controls to prevent unauthorized access and modification to the LAN, its resources and the information it transmits.

A. Reviewed security plans, security policies and procedures and risk analyses for the LAN to identify vulnerabilities and to determine the types of information that need to be exchanged between servers.

B. Reviewed access path diagrams to identify entry points into the LAN and selected systems, and determined if the entry points are adequately controlled.

C. Determined if any trusted relationships exist between the LAN and other networks. If so, evaluated the adequacy of controls over these connections.

D. Obtained system access with limited user capabilities and tested whether we could access files or perform functions beyond the limited capabilities.

E. Observed whether users stored data on personnel computers, and whether file-level controls properly restricted access to the file owners.

F. Determined if a workstation locking mechanism is available to prevent entry into the LAN when users leave their work area. Observed user demonstration of the locking device. Determined whether users are either automatically logged-off the system or the users' terminals are automatically locked after a specified period of inactivity. Observed employees' utilization of the system locking mechanism.

G. Determined if sensitive data is transmitted over the LAN medium. If so, determined whether it is protected from compromise by the use of encryption or some other data integrity service.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Richard T. Hayes, Audit Manager
Gerald H. Horn, Audit Manager
Bret Hunter, Senior Auditor
Joan Raniolo, Senior Auditor
Billy Benge, Auditor
David Hodge, Auditor
Midori Ohno, Auditor
Una Smith, Auditor
Theodore Tomko, Auditor

Appendix III

Report Distribution List

Director, Office of Security and Privacy Oversight IS:SPO
Director for Legislative Affairs CL:LA
Office of Management Controls CFO:A:M
Office of Chief Counsel CC
Director, Office of Program Evaluation and Risk Analysis M:O
National Taxpayer Advocate C:TA
Director, Information Technology – Midstates Area IS:F:MS
Director, Houston District
Audit Liaison: Chief Information Officer IS