The Internal Revenue Service Can Improve Software-Based Access Controls to Enhance Security for Local Area Networks

April 2000

Reference Number: 2000-20-073

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

April 28, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Can Improve Software-Based Access Controls to Enhance Security for Local Area Networks

This report presents the results of our reviews to assess the adequacy of the Internal Revenue Service's (IRS) software-based access security (also known as logical control) for its local area networks (LANs). This audit was part of a series of reviews initiated to assess the overall effectiveness of security controls over the IRS' information systems. Related reviews covered operational/ telecommunications security and physical security, which will be reported on separately. We issued a draft of this report to IRS management on March 20, 2000 with an April 20, 2000 response period. However, management's response was not available as of the date this report was released.

In summary, the IRS does not have uniform minimum security standards for software-based access protection of its LANs. Although the IRS has drafted logical control standards for Windows NT operating systems, it has not mandated adherence to these draft standards. In implementing its LAN security program, the IRS needs to: 1) apply policies and guidance that restrict logical access to specific data and resources, 2) install necessary controls over individual users of information systems data and resources, and 3) produce and analyze audit trails for all necessary system and user activity.

To address these conditions we recommended that the Chief Information Officer, in conjunction with other IRS executives, assign responsibility for planning, implementing and maintaining minimum logical access security measures for the IRS' information and data residing on LANs. These actions should include developing and adopting uniform logical security standards and guidelines, and having the Office of Security and Privacy

Oversight (previously known as the Office of Security Standards and Evaluation) conduct reviews to determine whether the prescribed logical access security guidelines are in place.

Please contact me at (202) 622-6510 if you have questions, or your staff may call Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Executive Summary

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, computer security helps the organization’s mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

To accomplish its mission, the Internal Revenue Service (IRS) relies heavily on computers linked together in a vast collection of networks, known as Local Area Networks (LAN). Because of the IRS’ heavy reliance on computers, effective controls are critical to maintain confidentiality of taxpayer data, safeguard assets, and ensure the reliability of financial management information.

Control components for computer LANs include software-based security provisions (also known as logical access controls) and the supporting policies, organization, and procedures to protect computer-based data from unauthorized destruction, manipulation, or disclosure. The IRS has increased the use of LANs by its operating functions (e.g., Examination, Collection, Appeals, etc.). This increase in LANs has led to the need for logical access security controls, such as passwords and restrictions on user access to applications, files, and data. These controls help prevent loss, inappropriate use and unauthorized disclosure of information.

The overall objective of this review was to assess the adequacy of software-based (logical) access controls used to assure sufficient security for the IRS’ information systems and sensitive data residing on its LANs. This review was part of a series of reviews initiated to assess the overall effectiveness of security controls over the IRS’ information systems. Related reviews covered operational/telecommunications security and physical security, which will be reported separately.

Results

The IRS, as well as the Congress and the General Accounting Office (GAO), recognize the risks and vulnerabilities associated with the scope and magnitude of the IRS’ information systems security. Along with the IRS’ own self-assessments, the GAO recently issued reports about the IRS’ information systems security. The GAO related in its report entitled *IRS Systems Security* (GAO/AIMD-99-27, December 1998*)* that although the IRS has made significant progress to improve security at IRS facilities, serious weaknesses persist.

The IRS has taken considerable steps to improve its computer security program, including enhancing its logical, physical and telecommunications access security

measures for LAN systems and data. However, assessing and reducing risks at over 1,000 IRS facilities is a significant undertaking. We found that the IRS has not implemented uniform minimum security standards for logical protection of its LANs. Logical control standards for its LANs using the Windows NT operating systems have been drafted, but not mandated.

By Providing Policies and Guidance the Internal Revenue Service Can Properly Restrict Access to Computer Data and Resources

This review identified the following weaknesses in policies, procedures, practices and conditions that hinder the IRS from achieving adequate logical access security for data residing on its LANs.

- The IRS has not implemented all necessary controls that restrict access to LANs, servers and workstations. Providing necessary access controls for LANs can prevent inadvertent or malicious tampering with the IRS' software programs or data. Specifically, access by unauthorized personnel at the LAN, server, and workstation levels can result in interruptions of the IRS' operations, inappropriate management of taxpayer account actions and data, and improper disclosure of sensitive taxpayer information.
- The IRS does not have all necessary controls over individual users of LAN systems and data. The IRS does not always verify that only authorized users have LAN access, and that access capabilities are authorized. Also, the IRS does not have current information access and disclosure agreements with contractors to protect sensitive data. In operating its LANs, the IRS does not require employees to log off computers they are not using. These conditions can allow unauthorized access to computer applications or data.
- The IRS does not produce and analyze audit trails for all necessary LAN and user activity. Audit trails provide information on LAN and application process actions, as well as user activity on LANs and applications. Only two of the IRS' operating divisions record and review their LAN audit trail information on a national basis, and these functions review only user accesses to the LANs or applications. None of the IRS' operating divisions conduct reviews to identify the particular transactions the users accomplished on LANs and applications. Without some form of transaction review, users' inappropriate actions will go undetected.

Addressing these weaknesses will improve LAN security. This involves assessing and managing available resources to address the existing and potential security threats.

Summary of Recommendations

The Chief Information Officer (CIO), in conjunction with other IRS executives, should assign responsibility for planning, implementing and maintaining minimum logical access security measures for the IRS' information and data residing on LANs. These actions should include developing and adopting uniform logical security standards and guidelines, and having the Office of Security Standards and Evaluation conduct reviews to determine whether the prescribed logical access security guidelines are in place.

These guidelines should include provisions that require a periodic comparison of LAN users to current personnel records to ensure that only authorized users access the IRS' LANs. The IRS also needs to enforce requirements to periodically review and update system records that identify and authorize its LAN users, including having current access and disclosure agreements with contractors.

As a means to prevent access to LAN computer workstations by unauthorized users, these guidelines should require the use of automated features, such as password protected screensavers.

Finally, the CIO and other IRS executives should develop and implement audit trail policies for computer LANs and define the levels that need review (i.e., LAN, server level, and/or workstation level).

Management's Response:

We issued a draft of this report to IRS management on March 20, 2000 with an April 20, 2000 response period. However, management's response was not available as of the date this report was released.

Objective and Scope

Software-based security provisions and the supporting policies, organization, and procedures that protect computer-based data from unauthorized destruction, manipulation, or disclosure are known as logical access controls. To assess the adequacy of the IRS' information systems security we considered control objectives for logical access security.

The overall objective of this review was to assess the adequacy of software-based (logical) access controls used to assure sufficient security for the Internal Revenue Service's (IRS) information systems and sensitive data residing on local area networks (LANs). Logical access security ensures taxpayer information is properly secured and protected through control of systems users and resources, separation of duties for computer personnel and use of audit trails.

To accomplish our objective, we visited 24 IRS sites between March and May 1999. The IRS sites we visited had varying operations and geographical makeup. We performed these reviews in accordance with *Government Auditing Standards* in the following types of facilities: computing center, service center, service center post of duty, software development center, district office headquarters, and district office post of duty.

We reviewed logical access security in different types of IRS facilities in 24 sites around the nation.

We focused our reviews on identifying and analyzing the IRS' security control structure and existing security procedures surrounding logical access security measures on LANs. This review included only limited transaction testing of logical control and access related activities.

Details of our audit objectives, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II. Appendix IV presents a glossary defining technical terminology used in this report.

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.

To accomplish its mission, the IRS relies heavily on computers linked together in a vast collection of networks, known as Local Area Networks (LAN). The risk to computer security increases as the number and complexity of these connections and LANs grow.

Because of the IRS' heavy reliance on computers, effective controls are critical to maintain confidentiality of taxpayer data, safeguard assets, and ensure the reliability of financial management information.

The IRS depends on computers to process over 200 million taxpayer returns and collect over $1.7 trillion in taxes annually. The IRS also operates hundreds of other facilities (e.g., regional, district, and outlying offices) that support tax processing.

Major computer systems used for processing tax return information located at the IRS' large facilities generally include mainframes and mini-computers. The IRS also operates administrative applications on mini-computers located in regional and district offices. Outlying field offices have access to applications operating on mini-computers. These locations integrate computer systems and applications with networking capabilities.

Physical controls can help in protecting the data stored and processed on networked computer systems. Providing security for data when computers are interconnected in LANs, however, requires more than physical controls.

The increase in use of LANs by the IRS' operating divisions (e.g., Examination, Collection, Appeals, etc.) has led to the need for logical (software-based) security controls such as passwords, and restrictions on user access to applications, files, and data.

Logical security controls enable organizations to:

- Restrict access to LANs, servers and workstations.
- Identify individual users of computer data and resources.
- Produce and analyze audit trails of system and user activity.

The IRS, as well as the Congress and the General Accounting Office (GAO), recognize the risks and vulnerabilities associated with the scope and magnitude of the IRS' computer security. Along with the IRS' own self-assessments, the GAO recently issued reports about the IRS' computer information systems security. The GAO related in its report entitled *IRS Systems Security* (GAO/AIMD-99-27, December 1998*)* that although the IRS has made significant progress to improve computer security at its facilities, serious weaknesses persist.

The Congress recognized the significance of maintaining adequate computer systems security in the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98)[1]. This law directs the Treasury Inspector General for Tax 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

Federal law, Department of Treasury directives and the IRS' own internal policies and procedures require the implementation of sound computer security practices. The IRS has taken considerable steps to improve its computer security program. These steps include the creation of the Office of Security Standards and Evaluation (SSE). In 1998, the SSE began performing computer security risk assessments at the IRS' facilities nationwide. In addition to the risk assessments, the SSE is working with IRS management to correct security weaknesses identified. However, assessing and reducing risks at over 1,000 IRS facilities cannot be completed in a few years. It is a progressive and continuous process.

Although the IRS has taken steps to further secure its computer security, it does not consistently apply logical

[1] P.L.105-206, 112 Stat. 685 (1998)

access security measures throughout all of its LAN operations. Specifically, the IRS needs to accomplish the following to meet minimum computer security standards:

- Develop policies and guidance to restrict user access to specific data and resources.
- Provide necessary controls over individual users of computer data and resources.
- Produce and analyze audit trails of system and user activity.

These improvements will reduce the effects of exposures in computer security. Eliminating or reducing these exposures involves assessing and managing available resources to address the existing and potential security threats.

Appendix V presents a table of the specific security exposures identified during this review. The table presents the security exposures by IRS facility type and responsible operating and/or support division.

By Providing Policies and Guidance the Internal Revenue Service Can Properly Restrict Access to Computer Data and Resources

Logical access controls are the computer-based means by which users are allowed or restricted access to applications, files, and data. Logical access controls can prescribe not only who can access specific systems or data, but also the type of access that is permitted.

The IRS has not implemented uniform minimum security standards for logical protection of its LANs. Although the IRS has drafted logical control standards for LAN computers using Windows NT operating systems, it has not mandated adherence to these standards.

The IRS Needs to Implement Controls That Restrict Access to LANs, Servers and Workstations

Limiting access to LANs is necessary to ensure continued operations. Restricted access prevents intentional or accidental changes to LAN and application configurations, as well as the destruction or manipulation of data. The IRS does not consistently apply the following controls that are necessary to meet minimum computer security standards.

The IRS needs to implement logical access controls that only allow appropriate people access to networks, servers and workstations.

- Renaming all vendor supplied accounts named "administrator" in software applications. This process reduces the risk of an unauthorized user gaining access to a computer by using the name "administrator," which can provide an unauthorized user complete control of a LAN computer (full network administrator rights).
- Denying users the ability to access a LAN computer without a password (blank password). Eliminating this free access ability reduces the risk of unauthorized access. This provision also prevents inadvertent or malicious tampering with computer software programs or data.
- Denying, limiting or monitoring LAN administrator access to highly sensitive information such as grand jury, criminal case, or audit trail information. The IRS does not have formal guidance and controls for access to this data. Controls over LAN administrator access to this data reduces the risk of data tampering and unauthorized disclosure of information, which could lead to legal issues and negative perceptions from the public.
- Denying users the ability to use LAN server workstations, and the ability to modify security-related provisions on their own computers. These provisions prevent users from inadvertently or maliciously tampering with LAN system software programs, data and security-related provisions.

Uniform standards for logical security controls will provide guidance for systems administrators to protect the access to their systems.

The majority of LAN administrators we interviewed indicated that they were not aware of formal logical security guidelines. Two LAN administrators indicated that they referred to their own locally developed security guidelines.

Improvements in logical access controls to LANs and applications will allow the IRS to enhance its overall level of computer security. The above requirements only begin to encompass the opportunities to protect LANs and the related computers and data. Suggestions for minimum security configurations of LANs can be easily found in government publications, books that publish industry "best practices" standards, and the Internal Revenue Manual.

The Internal Revenue Service Needs to Provide Necessary Controls over Individual Users of Computer Data and Resources

The American Society of Industrial Security estimated that insiders commit 77 percent of information theft.

In many computer security surveys and studies, managers, security experts and readers express concerns that internal employees present the greatest threat to their computer systems. The American Society of Industrial Security estimated that insiders commit 77 percent of information theft. Internal employees are familiar with the LANs, know which systems hold valuable information, and may have easy access to those systems through their own account or the account of a co-worker. In addition, internal employees have physical access to LAN hardware components. Internal employees include contractual partners, such as technical advisors and janitors.

Improvements in controls over internal LAN user access capabilities will allow the IRS to enhance its ability to ensure only authorized people use its computer systems. These controls also focus users on their security responsibilities through automated warnings to protect sensitive data such as tax return information.

The IRS does not consistently apply the following controls that are necessary to meet minimum computer security standards.

- Requiring employees to log off computers they are not using. This action prevents unauthorized users from accessing computer applications or data on another employee's computer.
- Verifying and updating records for all current LAN users. IRS managers should verify the validity of current authorized users along with their authorized system capabilities. This process will reduce the risk of unauthorized user access and/or transactions. Periodically validating current authorized users will identify users who no longer require access or whose access needs have changed.
- Obtaining current access and disclosure agreements with contractors who are working with the IRS' computer systems. These contractors should follow the same standards as employees to protect sensitive data and taxpayer information. Also, IRS management should ensure that all LAN computers display a Federal Government System warning message advising users to protect this data and information. These procedures provide additional assurance that all potential users know their security responsibilities and the legal importance of protecting taxpayer data.

As organizations focus on security from external threats, they often overlook security controls over internal employees.

The IRS has recognized the need for each of the above controls and has taken actions to use them. However, these controls are not uniform, always implemented, or strictly enforced.

For example, most LAN administrators we interviewed indicated that current LAN computers were set up with automated features that prevent unauthorized users from accessing another employee's computer (password protected screensavers). However, one LAN administrator disabled this feature. The LAN administrator believed that productivity could be negatively impacted by numerous sign-on actions required by employees. Specifically, this LAN administrator's productivity concern was that when employees left their workstations and subsequently returned, they would have to input their passwords to resume their work. In other instances, LAN administrators were not aware that employees disabled this feature.

Regarding validation of authorized users, all sites we visited used some form of notification for employees who have left the IRS. The most common practice involved using a bi-weekly report, from the personnel office, listing recently separated employees. In most of the sites, LAN administrators did not follow up to ensure the employees were properly prevented from using the systems. We found employees who separated from the IRS that continued to have access to the IRS' LANs. Specifically, we found twelve employees who had the potential for continued access up to five months subsequent to their separation. Because of an absence of records, actual access by separated employees was not possible to determine.

Regarding validation of user capabilities, we found two instances where LAN users were not aware that they had the means to add, delete or alter other users' access to the LAN.

The Internal Revenue Service Needs to Produce and Analyze Audit Trails for All Necessary Computer and User Activity

Audit trails provide information required to trace or re-create a sequence of events and can assist IRS management in detecting security violations.

Audit trails provide information on system and application process actions, as well as user activity on LAN systems and applications. Only two of the IRS' operating divisions record and review their LAN audit trail information on a national basis. These operating divisions only perform reviews of user accesses to the LANs or applications. None of the IRS' operating divisions conduct reviews to identify the particular transactions the users accomplished on LANs and applications. Without some form of transaction review, inappropriate user actions will go undetected.

Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

The Internal Revenue Manual requires LAN administrators to generate and distribute audit trails to appropriate managers for review. However, the Internal Revenue Manual does not specifically identify which systems require review, or the most practical level of the system that should have audit trails reviewed (LAN, server, or computer). As a result, field managers have interpreted their own specific responsibilities on the use of audit trails. For example, we only found one division that reviewed audit trails. This review was locally initiated and limited to their LAN servers. In other sites managers expressed that they are awaiting direction, education and instruction from the IRS National Office for generating and reviewing audit trails.

Recommendation

1. The CIO, in conjunction with the IRS' executives and managers, should develop and adopt uniform logical security standards and guidelines for computers and information residing on LANs. Subsequent reviews conducted by SSE should determine whether the IRS implemented the security standards and guidelines as prescribed.

   These guidelines should include the following provisions.

   – Require employees to log off computers they are not using. Additionally, guidelines should be developed to use automated features that prevent access to LAN computers by other users (automated password protected screensavers).

     The guidelines should specify a standard amount of time for screensaver activation that does not exceed 15 minutes.

   – Require periodic review and update of records that identify, authorize, and register the IRS' computer users. Records should include Forms 5081, Automated Information Systems User Registration/Change Request Preparation Instructions, or similar formal written or electronic records, and current access and disclosure agreements with contractors.

- Require a periodic comparison of computer users to current personnel records. This comparison allows managers of LANs to identify users of their systems who are not current IRS employees, and current employees who no longer need access to their system.
- Require all LAN computers to display a Federal Government System warning message advising users to protect all sensitive data and information. These procedures provide additional assurance that all potential users know their security responsibilities and the legal importance of protecting taxpayer data.
- Develop and implement audit trail policies that identify LANs and define the levels that should be reviewed (LAN, server, and/or individual computer). Once the policy is devised, the IRS needs to allocate resources to determine what information to capture; capture the information; and educate reviewers to interpret audit trail information.

Management's Response:

Management’s response was not available as of the date this report was released.

Conclusion

The IRS needs to implement policies and controls to provide consistent security measures throughout its LAN computer operations. These measures can help prevent outsiders from breaking into LANs, and limit the effects of malicious acts by employees.

Vigilance in implementing and maintaining this LAN security program will help the IRS meet its mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

Implementation of our recommendations could reduce: 1) delays in processing and collecting taxes as a result of breaches in security, 2) opportunities to improperly manipulate or destroy program data, 3) opportunities for theft, and 4) 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 assess the adequacy of software-based (logical) access controls used to assure sufficient security for the Internal Revenue Service's (IRS) systems and sensitive data residing on local area networks (LANs). To accomplish our objective, we:

- Analyzed the development and communication of the IRS' policies and guidelines, computer security plans including risk assessments, and certifications.
- Reviewed the IRS' information systems oversight including reviews performed by the Office of Security Standards and Evaluation (SSE).
- Performed tests and observations of controls in the IRS facilities identified below.

The review objectives considered logical access security controls over major IRS information systems to ensure taxpayer information is properly secured and protected through control of systems users and resources, separation of duties for computer personnel and use of audit trails.

We performed these reviews in the following types of IRS facilities:

- Computing Center - 1
- Service Center - 1
- Service Center Post of Duty -2
- Software Development Center - 1
- District Office Headquarters - 3
- District Office Post of Duty (with computer room) - 3
- District Office Post of Duty (without computer room) – 13

IRS Facilities Reviewed:

- Computing Center: Tennessee Computing Center
- Service Center: Memphis Service Center
    - Service Center Posts of Duty / Host Sites:
      Lamar site - Memphis, Tennessee
      Mendenhall site - Memphis, Tennessee
- Software Development Center: Las Vegas Development Center
- District Office: Los Angeles District
  - District Office Headquarters: Los Angeles, California
    - District Office Posts of Duty (without computer room):
      El Monte, California
      El Segundo, California
      Glendale, California
      Monterey Park, California
      Thousand Oaks, California
      Van Nuys, California
      Woodland Hills, California
- District Office: Manhattan District
  - District Office Headquarters: Downtown Manhattan - New York, New York
    - District Office Post of Duty (with computer room):
      Midtown Manhattan - New York, New York
    - District Office Post of Duty (without computer room):
      Bronx - New York, New York
- District Office: Southwest District
  - District Office Headquarters: Phoenix, Arizona
    - District Office Posts of Duty (with computer room):
      Las Vegas, Nevada
      Albuquerque, New Mexico
    - District Office Posts of Duty (without computer room):
      Northwest Phoenix, Arizona
      Tempe, Arizona
      Tucson, Arizona
      Reno, Nevada
      Santa Fe, New Mexico

Audit Objectives and Tests

I. To determine whether the IRS effectively developed and communicated computer security policies and guidelines, including Internal Revenue Manual (IRM) sections, Information Systems standards and procedures, and high level operational guidelines, we:

A. Interviewed staff from the offices of the Chief Information Officer (CIO), Director of Real Estate Planning and Management and Regional Directors of Information Systems to identify policies and guidelines used to implement and maintain security for computing centers, service centers, and district/regional computer facilities.

B. Interviewed Regional Field Information Systems Office (FISO) executives, site security managers, and obtained security related correspondence from the National Office to determine whether the security policies and plans were adequately communicated.

C. Obtained and reviewed the Office of Systems Standards and Evaluation (SSE) reviews. Determined the depth and scope of its reviews.

II. To identify current guidelines and standards for Federal Government information systems, we reviewed and analyzed the following documents containing industry/government information systems security standards:

- Office of Management and Budget Circular A-130
- National Institute of Standards and Technology's Generally Accepted Principles and Practices for Securing Information Technology Systems
- Department of Justice's "Vulnerability Assessment of Federal Facilities"
- Institute of Internal Auditors' "Systems Auditability and Control"
- Information Systems Security Procedural Guide (IRS Document 9627)
- IRS Windows NT Security Guidelines
- Consolidated Physical Security Standards for IRS Facilities
- The IRM.

III. To evaluate the adequacy of logical security controls over systems users and resources we:

A. Determined if Information Systems' (IS) personnel maintain an inventory that identifies all systems providing access to the IRS Data Communications Utility (DCU) through hardware they control, and verified whether all systems were certified through the Certification Office.

B. Verified, in each site visited, whether local IS management incorporated IRM requirements and industry best practices for:

1. Validating systems user account inventory with personnel records.
2. The principle of least privilege (e.g., granting the minimum access authorization necessary for performance required tasks) for the regular user's and systems administrator's rights and for file level accesses.
3. User account lockout tolerance (e.g., lockout after 5 unsuccessful attempts), lockout reset time (e.g., reset count after 10 minutes) and lockout duration (e.g., lockout for 30 minutes).
4. Password age (e.g., change frequency includes minimum of 1-5 days and maximum of 45-90 days), and password strength (e.g., 6 or more characters).
5. Accountability for systems administrator (e.g., employee and application) passwords and accounts.

C. Interviewed local IS management to identify recently transferred employees and verified that:

1. Security personnel were given notice of the terminations.
2. Identities and passwords were promptly revoked.
3. Computer room keys were returned and/or combinations changed.

D. Determined whether confidentiality or security agreements were on file for contractors assigned to work with confidential information.

E. Selected a sample of users including dial up access users (application and IS personnel), and reviewed access authorization documentation (Form 5081 or similar form) to determine if they had been properly approved by appropriate IRS management and transferred to the security function.

F. Physically observed workstation sign-on procedures for a sample of available users, including server workstations, to assure that:

1. The last user's name is not displayed on the login screen.
2. Passwords were not displayed in clear text.
3. Password protected screen savers were enabled and set to come on within 15 minutes.

4. An appropriate warning message was visible at the log-on screen.

G. Determined if an individual had been appointed Security Plan Coordinator for their respective organization.

H. Determined if an individual(s) had been designated as responsible for implementing the general policies over system security.

I. Interviewed local IS management to determine:

1. If there was a formal procedure for identifying employee training needs.
2. If there was a formal procedure for obtaining the necessary training resources.
3. What alternative training methods they support when funding was limited.

J. Reviewed information systems incident reports to determine the frequency of questionable transactions attributable to the uncertified systems.

IV. To determine the effectiveness of controls for separation of duties over Information Systems personnel, we:

A. Interviewed IS systems administrators, programmers, security analysts, functional coordinators, and managers to determine the extent that they have access to the machine log files and audit trails.

B. Interviewed IS purchasing agents, programmers, systems administrators, security analysts, functional coordinators, and managers to determine the extent that they have access to the inventory database.

C. Interviewed IS office programmers, systems administrators, security analysts, functional coordinators, and managers to determine the extent that they have approval authority and systems administrator capability to add or delete users from the system.

D. Interviewed managers and determined if reviews are conducted to assure user account transactions they approve are completed.

E. Evaluated manager review procedures for validation of user account changes, and inventory changes.

F. Interviewed managers to determine if they identify and monitor activities of employees who have system’s administrator, security and inventory responsibilities.

G. Reviewed IS incident reports to identify activities associated with users who could not be identified as a current or former employee.

V. To determine if controls were effective for audit trails, we:

A. Determined if audit trails were generated and distributed to IRS management for review.

B. Determined what parameters are considered for audit trail reviews that were conducted.

C. Interviewed IS managers, IS personnel and security personnel to determine what training they have received to review audit trails.

D. Determined whether IRS management identified, investigated, and resolved audit trail security violation issues.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Scott A. Macfarlane, Director
Edward A. Neuwirth, Audit Manager
Eulala Davis, Senior Auditor
William Lessa, Senior Auditor
Glen Rhoades, Senior Auditor
William Tran, Auditor
Louis Zullo, Auditor

Appendix III

Report Distribution List

Chief Information Officer IS
Assistant Commissioner IS Field Operations IS:FO
Assistant Commissioner National Operations IS:O
Assistant Commissioner Service Center Operations IS:SC
Director, Office of Security and Privacy Oversight IS:SPO

Appendix IV

Glossary of Terms

Administrator (Network/System) - A person who manages a communications network within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program and providing for routine backups.

Application - A specific use of the computer, such as for payroll, inventory and billing.

Audit Trails - A record of transactions in an information system that provides verification of the activity of the system.

Blank Password - An access configuration where a user is not required to input typed characters representing a typical password, to log on or gain access to a network.

Certification - The technical evaluation, made as part of and in support of the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements.

Confidentiality - Privacy of data during transmission, processing, or storage, usually through encryption or data separation.

Default - The current setting or action taken by hardware or software if the user has not specified otherwise.

Detection - Comparing normal patterns of behavior and identifying abnormalities that could be intrusions; the process of identifying that an intrusion has been attempted, is occurring, or has occurred.

Domain - In a communications network, all resources under the control of a single computer system.

File Server - A high-speed computer in a network that stores the programs and data files shared by users. It acts like a remote disk drive. The difference between a file server and an application server is that the file server stores the programs and data, while the application server runs the programs and processes the data.

Guest Account - A default set of permissions and privileges given to non-registered users of a system or service.

Local Area Network (LAN) - A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link.

Logical Access Security - Logical security includes software-based security provisions and the supporting policies, organization, and procedures to protect computer-based data from unauthorized destruction, manipulation, or disclosure.

Log off - To quit, or sign off, a computer system.

Mainframe Computer - There are small, medium and large-scale mainframes, handling from a few to tens of thousands of online terminals. Large-scale mainframes support multiple gigabytes of main memory and terabytes of disk storage. Large mainframes use smaller computers as front-end processors that connect to the communications networks.

1. A mainframe provides enormous amounts of throughput by offloading its input/output processing to a peripheral channel, which is a computer in itself. Mainframes can support hundreds of channels, up to 512 in some models. Mainframes also have multiple ports into memory and especially into high-speed caches, which can be 10 times faster than main memory. Additional computers may act as input/output traffic cops between the central processing unit (CPU) and the channels and handle the processing of exceptions (what happens if the channel is busy, if it fails, etc.). All these subsystems handle the transaction overhead, freeing the CPU to do real "data processing" such as computing balances in customer records and subtracting amounts from inventories, the purpose of the computer in the first place.
2. The internal bus transfer rates of mainframes are also higher than small computers.
3. Much of the hardware circuitry in a mainframe is designed to detect and correct errors. Every subsystem is continuously monitored for potential failure, in some cases even triggering a list of parts to be replaced at the next scheduled downtime. Consequently, mainframes are incredibly reliable. The mean time between failure (MTBF) is generally 20 years.

In addition, mainframes are highly scalable. Based on symmetric multiprocessing (SMP), mainframes can be expanded by adding CPUs to a system or by adding systems in clusters.

Network - A network is composed of communications media and all components attached to them. These components may include computers, routers, multiplexers, switches, transmission systems, and management and support services.

Network Administrator - See systems administrator.

Operating System - The master control program that runs the computer. It is the first program loaded when the computer is turned on, and its main part, called the kernel, resides in memory at all times.

It is an important component of the computer system, because it sets the standards for the application programs that run in it. All programs must "talk to" the operating system.

The main difference between an operating system and a network operating system is its multi-user capability. Operating systems, such as Macintosh System 7, DOS and Windows, are single user systems, designed for one person at a desktop computer. Windows NT and UNIX on the other hand are network operating systems, because they are designed to manage multiple user requests at the same time.

Operational and Physical Security - Operational security and physical security includes an established control structure that effectively manages and protects the integrity, confidentiality, and availability of information systems data and resources.

Password - A protected word or string of characters that identifies or authenticates a user for access to a computer system, or a specific resource such as data set, file or record.

Primary Domain Server/Controller (PDC) - In a Windows NT Server domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC.

Systems Administrator - A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A systems administrator would perform systems programmer activities with regard to the operating system and other network control programs.

Telecommunication Security - Telecommunications security includes not only the technology supporting the communication, but also the people, policies, and procedures that are critical to the success of telecommunications.

Users - People or processes accessing an automated information system (AIS) either by direct connections (i.e., via terminals) or indirect connections.

User Account - An established relationship between a user and a computer, network or information service. User accounts require a username and password, and new user accounts are given a default set of permissions.

Appendix V

Security Exposures by Internal Revenue Service Facility Type and Function

The following table depicts the specific security exposures identified in the Internal Revenue Service (IRS) facilities visited. The table presents the:

- Security Exposure
- Type of Facility Which Had the Exposure
- IRS Function Responsible for Managing the Risk Associated with the Exposure
- Reference to the Guideline/Criteria for Providing Adequate Measures to Provide Information Systems Security

The table includes the following abbreviations:

EP/EO - Employee Plans and Exempt Organizations
IRM - Internal Revenue Manual
POD - Post of Duty
NIST - National Institute of Standards and Technology
IIA - Institute of Internal Auditors guidelines for Systems Auditability and Control
IBM - International Business Machines Corporation
Doc. 9627 – Information Systems Security Procedural Guide

SECURITY EXPOSURE	IRS FACILITY			RESPONSIBLE FUNCTION							REFERENCE
	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
LOGICAL ACCESS SECURITY											
Restricting Access to Specific Data and Resources:											
A default "administrator" account was not renamed or removed, or "guest" accounts were not disabled after their use was no longer needed.	X	X	X	X				X			IRM 2.1.10.9.7
The primary domain server/controller allowed users the option to access network workstations without using passwords, and did not provide for account lockout or password expiration.	X	X	X	X		X	X				IRM 2.1.10.9.7
Workstations using "Windows for Workgroups" and "Microsoft Windows 95" allow unobstructed system access.	X	X	X	X	X	X	X	X			IRM 2.1.10.4.3.1
Restricting Access to Specific											

SECURITY EXPOSURE	IRS FACILITY			RESPONSIBLE FUNCTION							REFERENCE
	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
LOGICAL ACCESS SECURITY											
Data and Resources:											
Physically accessible servers did not have logical controls to prevent system user access.	X		X	X							IRM 2.1.10.4.6
Criminal Investigation network administrators have unrestricted access to grand jury and criminal case information.		X							X		Doc 9627 Chapter 5
Systems user accounts were not compared to the current on rolls personnel records.	X	X		X		X		X	X		IRM 2.1.10.4.1.9
Forms 5081 did not reflect current network users and their access capabilities.	X	X		X							IRM 2.1.10.4.11
Controls Over Users:											

SECURITY EXPOSURE	IRS FACILITY			RESPONSIBLE FUNCTION							REFERENCE
	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
LOGICAL ACCESS SECURITY											
All workstations did not restrict regular user access to other user accounts and modifications to security-related provisions on Local Area Networks (LAN).			X						X	X	Doc 9627 Chapter 5
Telecommunications specialists had domain administrator rights.	X			X							Doc 9627 Chapter 5
Some users had rights they were not aware of - system user profiles allowed the ability to change account properties of other users.		X		X							IRM 2.1.10.4.1.9
Evidence was not available showing that contractors had appropriate security disclosure agreements.		X		X							IRM 2.1.10.1.4.13
Controls Over Users:											

SECURITY EXPOSURE	IRS FACILITY			RESPONSIBLE FUNCTION							REFERENCE
	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
LOGICAL ACCESS SECURITY											
Network workstations did not display a Federal Government System warning message.	X		X	X							NIST P. 39
Employee workstations were active and left unattended.	X	X	X	X	X	X	X				IRM 2.1.10.9.7
Activated IBM workstations with continuous access to the IBM mainframe computer were left unattended. *	X			X							IRM 2.1.10.9.7(6)
Password protected screen savers were not set to activate within 15 minutes when the computers are idle.	X	X	X	X	X	X	X	X	X	X	IRM 2.1.10.4.5
Audit Trails:											

SECURITY EXPOSURE	IRS FACILITY			RESPONSIBLE FUNCTION							REFERENCE
	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
LOGICAL ACCESS SECURITY											
Not all network servers or workstation audit trails were activated.	X	X	X	X		X	X		X		Doc 9627 Chapter 5
Audit trails that were activated were not reviewed.		X	X	X		X	X	X		X	IRM 2.1.10.4.1.9
Network administrators/mainframe security analysts had unrestricted access to audit trail information. *	X	X	X	X		X	X	X	X		Doc 9627 Chapter 5

***** We also identified this security exposure in a Computing Center. Information Systems has functional responsibility for Computing Center operations.