The Internal Revenue Service Needs to Develop Security Policies for Local Area Networks

May 2000

Reference Number: 2000-20-074

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

May 3, 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 Needs to Develop Security Policies for Local Area Networks

This report presents the results of our review to assess the adequacy of the Internal Revenue Service's (IRS) security policies for local area networks (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 software-based access security controls (also known as logical 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 should improve security over LANs. Improvements include developing and implementing: 1) security plans for applications and systems residing on its LANs; 2) guidance for controlling access to LAN systems and applications; and 3) a strong security policy for configuring LAN telecommunication systems (routers). The IRS also needs to take steps to ensure that the guidance and procedures are fully implemented and standardized into everyday practices.

To address these conditions we recommended that the Chief Information Officer (CIO), in conjunction with Information Systems (IS) managers in field offices, develop and implement security plans for all systems residing on LANs. Security plan development should include certifying that LAN systems meet applicable minimum government security requirements. The CIO, in conjunction with IS field managers, should develop user's guides and operating manuals for each LAN system in operation. And, the CIO should clearly define the roles and responsibilities for the IRS' data telecommunication specialists and the contract vendor's technicians who interact with the IRS' LANs.

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

Federal law, Department of the Treasury directives, and the Internal Revenue Service's (IRS) own internal policies and procedures require the implementation of sound security practices. Although the IRS has taken steps to implement these laws, directives, policies and procedures, it needs to improve its security over Local Area Networks (LAN) by completing development of necessary controls, guidelines, and procedures. The IRS also needs to take steps to ensure these laws and directions are fully implemented and standardized into everyday practices.

The IRS has a very large and diverse inventory of computer systems, comprising approximately 84 mainframe computers, approximately 1,500 mid-range computers, and over 100,000 individual computers. Its wide area network includes approximately 1,200 LANs. The complexity of the IRS' technology creates many problems, including difficult control and security issues.

The overall objective of this review was to assess the adequacy of policies and guidelines used to establish sufficient security for the IRS' LANs and related telecommunication processes. 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 covering physical security and software-based access (logical access) security will be reported on separately.

Results

The IRS has recognized the importance of effective computer and LAN systems security. The Office of Security Standards and Evaluation (SSE) was created to oversee computer security. The SSE has focused its efforts in completing a risk management analysis. These efforts involve: 1) assessing risks and determining computer security needs at facilities; 2) working with the management of facilities and support functions to implement security policies and controls, which include action plans for prioritizing and obtaining resources for corrective actions; 3) developing and implementing awareness and training programs; and 4) performing follow-up reviews of facilities to monitor and evaluate success, and to reassess risks and needs.

This approach has helped the IRS identify and reduce the effects of computer security weaknesses and exposures at many IRS facilities. While the above actions help to reduce the security exposures at IRS facilities, the IRS has not developed overall policies and guidance for securing its LANs and related telecommunication processes. By focusing on specific exposures at facilities, rather than developing overall security policies, the

weaknesses identified by the SSE and the Treasury Inspector General for Tax Administration may continue or recur.

The Internal Revenue Service Should Improve Security over Local Area Networks

The following weaknesses in policies, procedures, and practices inhibit the IRS from achieving adequate security over LANs.

The IRS does not have security plans for applications and systems residing on its LANs

Without detailed security plans, the IRS cannot adequately assess and address the risks in operating LANs, such as potential loss, inappropriate manipulation, or improper disclosure of taxpayer or other sensitive information. A formal security plan can be used during risk assessments to identify LAN systems requiring modifications to meet minimum security standards. The security plan can also be used to ensure compliant LAN systems continue to meet security standards.

The IRS does not have documented guidance for controlling access to LAN systems and applications

System administrators, operators and Information Systems security staff require procedural guides to have knowledge of information systems operations and security controls. Users require a security guide to have knowledge of the security features provided by the information system, how they are used, and how they interact with one another.

The IRS does not have a strong security policy for configuring LAN telecommunication systems (routers)

Policies need to be developed to ensure that LAN telecommunication routers are configured to: 1) restrict access from outside the LAN; 2) prevent redirection of LAN traffic; 3) reduce the effect of disruption of service from outside intruders (denial-of-service attacks); and 4) maintain records of users access (audit trails).

Developing and properly implementing strong policies and guidance is a critical first step in improving security over the IRS' LANs. This involves assessing the risks and managing available resources to address the existing and potential security threats.

Summary of Recommendations

The Chief Information Officer (CIO) needs to develop policies and guidance to ensure that an adequate control structure and security program is in place to manage the IRS' LANs. To accomplish this:

- The CIO, in conjunction with field IS managers, should develop and implement security plans for all systems residing on LANs. Security plan development should include certifying that LAN systems meet applicable minimum government security requirements. Defining which systems and at what layer in the IRS (network, LAN, or server) requires applicable security plans is also an issue that the CIO and other IRS executives need to determine.
- The CIO, in conjunction with field IS managers, should develop user's guides and operating manuals for each LAN system in operation. These documents help ensure that the systems operate as designed.
- The CIO should clearly define the roles and responsibilities for the IRS data telecommunication specialists and the contract vendor's technicians who interact with the IRS' LANs. This will help maintain secure telecommunications for the IRS' LANs by preventing inappropriate access to sensitive information.

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

The overall objective of this review was to assess the adequacy of policies and guidelines used to establish sufficient security for the IRS' local area networks (LANs) and related telecommunication processes. We considered whether security policies for LANs were:

To assess the adequacy of security of the IRS' local area networks, we considered policies and guidance developed to address the operational and telecommunication components of LAN security.

1. Adequately defined, communicated, implemented and maintained.
2. Implemented timely, efficiently and economically.
3. Developed and implemented in accordance with applicable laws.
4. Adequately addressing the safeguarding of assets, including computer hardware and data.

We visited 24 IRS sites between March and May 1999. The IRS facilities 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 operational and telecommunications security in different types of IRS facilities in 24 sites around the nation.

We limited our reviews to the identification and analyses of security policies and existing procedures over the operational and telecommunication components of LAN security. We performed only limited transaction testing of telecommunication controls.

We defined the LAN security components we reviewed as follows:

<u>Operational Security</u> - the effectiveness of controls over support activities for major information systems located at the IRS' facilities. We reviewed the adequacy of policies and procedures available for systems administrators and users to implement LAN security measures.

<u>Telecommunications Security</u> - security controls over: 1) the IRS' LANs, including controls over network

hardware and software, such as firewalls, routers, and local communications ports; and 2) access to the Treasury Communications System (TCS) from inside and outside the Treasury firewall.

Details of our audit objective, 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. At present, the IRS has approximately 84 mainframe computers, 1,500 mid-range computers, and over 100,000 personal computers. Its wide area network (WAN) includes approximately 1,200 LANs. The risk to LAN security increases as the number and complexity of these connections grows. Because of the IRS’ heavy reliance on LAN systems, effective controls are critical to maintain confidentiality of taxpayer data, safeguard assets, and ensure the reliability of financial management information.

LAN security is a challenge for organizations to ensure continued operations. Risks to security originate from both outside attacks (hackers), and inside attacks (disgruntled or curious employees).

The IRS, along with other high-profile government agencies and corporations, is at risk from outsiders’ efforts to hack into LAN systems. Similarly, malicious acts by employees present an even greater risk since employees already have access to LANs, in addition to being physically located where the LAN hardware is housed.

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 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 size and scope of the IRS' information systems has demanded oversight and scrutiny about security of systems and data from within the IRS and by the Congress and the GAO.

The Congress recognized the significance in the need for maintaining adequate computer security in the IRS Restructuring and Reform Act of 1998.[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 the Treasury directives, and the IRS' own internal policies and procedures require the implementation of sound computer security practices. Although the IRS has taken steps to implement these laws, directives, policies and procedures, it needs to improve its security over LANs by completing development of a control structure with related guidelines and procedures. The IRS also needs to take steps to ensure these laws and directions are fully implemented and standardized into everyday practices.

By addressing these weaknesses, the IRS will reduce the effects of exposures to its LAN security. Eliminating or reducing these exposures involves assessing the risks and managing available resources to address the existing and potential security threats.

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

The Internal Revenue Service Should Improve Security over Local Area Networks

Although the IRS has taken steps to improve its computer security, the IRS' IS organization has not developed adequate security policies for systems residing on its LANs. These policies should provide security measures to prevent or reduce:

The IRS has implemented security steps to help ensure its computer security. However, it has not developed complete policies and guidance to provide overall security for the systems residing on its LANs.

- Unauthorized access to LANs, applications, and data.
- Loss or destruction of assets (hardware, software, data).
- Theft or misuse of assets (hardware, software, data).
- Loss of integrity, confidentiality and availability of systems.
- Introduction of undesirable software or programs.
- Interruptions in the continuity of operations and service.

The following weaknesses in policies, procedures, practices and conditions inhibit the IRS from achieving adequate security for its LANs. The IRS does not have:

- Security plans for the systems residing on its LANs. These plans require an assessment of risk in operating LANs throughout the IRS by identifying the inventory and location of systems requiring modifications to meet minimum security standards.
- Documented guidance for controlling access to LANs and applications. System administrators, operators, and IS security staff require a procedural guide (known as a Trusted Facility Manual) to have knowledge of LAN operations and security controls. Users require a Security Features User's Guide to have knowledge of the LAN security features, how they are used, and how they interact with one another.
- Telecommunication controls for LAN configurations that: 1) restrict access from outside the LAN; 2) prevent redirection of LAN traffic; 3) reduce the effect of disruption of service from outside intruders

(denial-of-service attacks); and 4) maintain records of users access (audit trails).

The SSE has reviewed and addressed computer security weaknesses at many IRS facilities. Although the SSE has helped improve security at these facilities, the IRS could continue to experience exposures to its LANs without an overall plan to meet minimum security standards.

The IRS has recognized the importance of computer and LAN security. The Office of Security Standards and Evaluation (SSE) was created to oversee computer security. The SSE has focused its efforts in completing a risk management analysis. These efforts involve: 1) assessing risks and determining computer security needs at facilities; 2) working with the management of facilities and support functions to implement security policies and controls, which include action plans for prioritizing and obtaining resources for corrective actions; 3) developing and implementing awareness and training programs; and 4) performing follow-up reviews of facilities to monitor and evaluate success, and to reassess risks and needs.

This approach has helped the IRS identify and reduce the effects of computer security weaknesses and exposures at many IRS facilities. The SSE's initial efforts focused on the IRS' larger processing facilities. Current efforts have focused on district offices and some of the districts' outlying posts-of-duty. The SSE has focused much of its effort in these reviews to reassess and correct computer security weaknesses identified by the GAO.

While the above actions help to reduce the security exposures at IRS facilities, the IRS has not developed overall policies and guidance for operating its LANs. By focusing on specific exposures at facilities, rather than developing and implementing overall LAN security policies, the security weaknesses identified by the SSE and TIGTA may continue or recur.

Appendix V presents a table of the specific security exposures we identified during our review. The table presents the security exposures by IRS facility type and responsible operating and/or support function. These specific exposures exemplify the need for policies and guidance that require implementation to provide adequate LAN security.

The IRS Does Not have Security Plans for Applications and Systems Residing on Its LANs

A security plan outlines responsibilities and expected behavior of all individuals who access the system.

The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, updated in 1996, and the Computer Security Act of 1987,[2] require security plans for all federal computer systems.

A security plan provides an overview of the security requirements of a system and describes the controls in place or planned for meeting those requirements.

All computer applications and systems must be covered by security plans if they are categorized as a *major application* or *general support system. Major applications* are required to have their own security plan. We did not assess the adequacy of *major application* security plans as part of our review scope.

General support systems are systems that provide support for a variety of users and applications. For example, a *general support system* can be a:

- LAN, including file servers and workstations, that support an area office.
- Communications network.
- Data processing center/customer service center including operating systems and utilities.

Standard commercial off-the-shelf software, such as Microsoft Office, is not considered a major application and should be covered by the plans for the general support systems on which they are installed.

A *general support system* normally includes hardware, software, information, data, applications, communications, facilities, and people. The Chief Information Officer (CIO) is responsible for ensuring that *general support system* security plans are developed and implemented for all IRS LANs and related applications, data, and communication systems.

The OMB Circular A-130, updated in 1996, now requires an assessment of risk as part of a risk-based approach in determining adequate, cost-effective security for a computer system. The methods used to assess the nature and level of risk to the system should

[2] Pub. L. No. 100-235, 100 Stat. 1724

include a consideration of the major factors in risk management:

- The value of the computer system or application.
- Threats.
- Vulnerabilities.
- Effectiveness of current or proposed safeguards.

The specific methods used should be described along with the date the risk assessment was conducted. Also, the assessment needs a statement on how the identified risk relates to the requirements for confidentiality, integrity, and availability determined for the system.

Assessing risk should be an on-going activity to ensure that new threats and vulnerabilities are identified and that appropriate security measures are implemented.

IS managers have not developed and implemented security plans for systems residing on the IRS' LANs. Reasons for this vary from site to site.

For example, the Field Information Systems Organization (FISO) Chief at one site stated she understood the need for a LAN security plan, but needed additional guidance on format and content. Conversely, the FISO Chief at another site stated that the development of a security plan is entirely the responsibility of IS at the National Office.
IS management at a third site requested that an outside contractor prepare the security plan.

On the other hand, Criminal Investigations (CI) unilaterally prepared and implemented a formal computer security policy that included a LAN risk assessment for its applications and systems. However, CI's security coordinators in field operations were not aware of the security policy and related risk assessment.

Until the IRS completes security plans for all *general support systems* in the field, LAN system vulnerabilities may go undetected, thereby jeopardizing the IRS' computing and processing operations, and exposing sensitive taxpayer data to unauthorized use, modification, and destruction.

Recommendation

1. The CIO, in conjunction with field IS managers, should develop and implement security plans for all *general support systems* residing on LANs, including clarifying roles and responsibilities. Security plan development should facilitate the certification of systems to meet applicable minimum government security requirements.

   The security plan establishes the system protection requirements and documents the security controls in the LAN. Thus, the security plan forms the basis for meeting minimum security requirements.

   A *general support system* security plan should contain the following elements:

   - System Identification.
   - Management Controls.
   - Operational Controls.
   - Technical Controls.

   Appendix VI presents a template of a *general support system* security plan. This template can be found in the National Institute of Standards and Technology (NIST), Guide for Developing Security Plans for Information Technology Systems, Special Publication 800-18, dated December 1998.

   Once completed, the appropriate information systems manager should forward the *general support system* security plan to the CIO for approval. After approval, the SSE should perform reviews to assess how well the plan was implemented.

<u>Management's Response</u>: Management's response was not available as of the date this report was released.

<u>The IRS Does Not Have Documented Guidance for Controlling Access to LAN Systems and Applications</u>

The IRS' information systems are formed through a large number of interconnected sub-systems that process sensitive but unclassified information, such as taxpayer information on tax returns and related documents. Various functions within the National Office and field office levels developed, own, and/or maintain these systems.

In the district office, service center and computing center we visited, none of the IRS functions had the following types of documented guidance to manage their LAN systems:

– System Certification and Accreditation.

– Trusted Facilities Manuals.

– Security Features Users Guides.

System Certification and Accreditation

Treasury Department Publication (TDP) 71-10, *Treasury Department Security Manual*, dated October 1, 1992, establishes the certification and accreditation policy.

Certification ensures LAN security measures are correctly implemented. Accreditation authorizes a system for operation with acceptance of any risk.

The Information Systems Certification is a formal review and test of the security safeguards implemented in the LAN system to determine whether the system meets security needs and applicable requirements. Certification is a method for ensuring that an appropriate combination of system security measures is correctly implemented to counter relevant threats and vulnerabilities.

Information Systems Accreditation is the formal authorization by the LAN system owner for operation of the system and acceptance of any security risks. Once accredited, systems must be re-certified at least every three years or when changes to the system occur that impact security such as:

- A change in security policy (e.g., access control policy).
- A change to the operating system or to software providing security features.
- A change to the configuration of the LAN system (e.g., a workstation is connected to the LAN outside of the approved configuration).

Without documentation of the accredited security requirements, IS managers do not have a reference for setting and maintaining minimum security standards when operating their LANs.

In all the sites we visited, networked workstations were in use with uncertified and possibly unsecured operating systems.

Operating systems on some LAN computers did not include security features to limit unauthorized access.

- One IRS function exclusively used Microsoft's Windows 95 operating system on all its workstations. A significant security weakness of this system is any user's ability to operate the computer by simply canceling the password and allowing unauthorized users access to applications and data.
- A limited number of computers in each of the district, service center and computing center offices visited used Windows 95, Windows 3.1, or DOS operating systems connected to a LAN. These systems do not meet minimum government security requirements for controlling access (known as C2 level security), again allowing unauthorized users access to applications and data.
- In one office all the security features of the operating system were disabled to accommodate DOS workstations with LAN connections. This system has been in an unsecured mode for more than two years.

The IRS has not determined whether the National Office or field offices have responsibility for obtaining certifications and developing security guidance. Without documentation of these security plans, the IRS has no assurance that minimum security measures are in place. The absence of guidance from the National Office has resulted in field IS managers interpreting their own security roles and responsibilities.

- In one case, a manager indicated that his LAN was nothing more than a component of the IRS' corporate network structure, so he did not have control over the security configurations.

- Several managers stated they assumed that the National Office IS staff completed certifications and development of information systems security related manuals.
- One manager was in the process of contracting out the certification of her LAN and development of security manuals.

Trusted Facility Manual

Systems Administrators need Trusted Facility Manuals for guidance on system security policies.

The IRS' Document 9627 (5/98), *Information Systems Security Procedural Guide*, requires a procedural guide (known as a Trusted Facility Manual) that gives specific guidance to system administrators on how to:

- Configure and install the LAN and related systems.
- Administer and operate the LAN in a secure manner.
- Make effective use of the system privileges and protection mechanisms to control access to applications and databases.
- Avoid risks and improper use of the applications that would compromise the sensitive system data and user security.

Without proper guidance, LAN administrators may not install or maintain desirable systems security settings.

In three offices we visited, regular users had the ability to access and operate the LAN server workstation. Using the LAN server as a workstation significantly increases the risk of unavailability of LAN services offered by the server. In one of these offices, all IRS employees located in the building had unmonitored physical access to the servers.

Most operating systems, such as Windows NT, come with default administrator account names and passwords that are common knowledge to many computer users. A system administrator's account allows access and control to system resources and data.

In two offices we visited, the network system administrator's default network account was not renamed to reduce the risk of unauthorized access.

Security Features User's Guide

A Security Features User's Guide provides users instruction in maintaining security while using computer systems.

Document 9627 also requires a Security Features User's Guide for each LAN that explains to users:

- What security features are provided by the system.
- How to use the security features correctly.
- How LAN systems interact with one another.

In all the offices we visited and in most of the functions that used LAN services, we found unattended employee workstations that were actively signed on to a LAN. An unattended computer logged onto a LAN gives anyone who has physical access to the computer complete access to the user files and all LAN services allowed to the user -- including Internet and e-mail services. Free access to workstations can result in unauthorized users improperly accessing, manipulating, or destroying sensitive information.

A Security Features User's Guide would provide the users information to assist them in following security procedures and reducing risks. For example, on some of the LANs, the computer operating system offered a security feature to automatically lock the workstation from use when left inactive for a specified amount of time. Only the person who was signed on to the workstation prior to it locking has the ability to unlock the workstation using his/her personal LAN password. We found that users generally do not use this feature.

In all offices, some systems in use did not offer an automatic terminal locking security feature. In these cases, the users need to know that signing off prior to leaving their workstations can reduce access risk.

Recommendations

2. The CIO, in conjunction with other IRS executives and field IS managers, should clearly define which level of networked systems require certification.

The guidelines should also identify the functional managers at both the National Office and field office levels responsible for assuring the systems are properly certified for operation.

3. The CIO, in conjunction with field IS managers, should develop Trusted Facility Manuals and Security Features User's Guides for each system in operation.

<u>The IRS Does Not Have a Strong Security Policy for Configuring LAN Telecommunication (Router) Systems</u>

A router is a computer that forwards information from one LAN or WAN to another. Routers allow users to access systems and data in various locations. Often this includes sensitive taxpayer information. Because these systems process and transmit sensitive data, routers should be configured to allow only authorized users access to sensitive data. Even for data that is not sensitive, appropriate measures must still be taken to ensure data are not lost, manipulated or improperly disclosed. To protect the privacy, integrity, and authenticity of this data, a strong security policy for LAN telecommunication (router) configurations needs to be established and enforced nationwide.

The IRS' facilities have security weaknesses in LAN telecommunication (router) configurations. Controls are not in place to:

- Prevent unauthorized users from accessing LANs.
- Reduce the effect of disruptions in service from outside intruders (denial-of-service attacks).
- Maintain system access histories (audit trails) of router traffic.

<u>LAN Telecommunication Access Controls</u>

A strong security policy must contain adequate controls to restrict router access only to authorized users.

In the offices we visited, routers were not configured to restrict inappropriate remote access from outside the LAN. Router configurations did not prevent access to other LAN systems by unauthorized employees. Any

IRS employee with valid network user identification and a network router address [i.e., Internet Protocol (IP) address] can access a router residing anywhere on the IRS WAN by obtaining a router password.

Hypothetically, a Los Angeles District Collection employee could obtain information about a Manhattan District taxpayer's audit status by accessing Manhattan District Examination Division's inventory records. With the router address and his/her own user identification, he/she could test password combinations until successful ("crack" the password) to gain network access.

A second type of access control deals with the unauthorized redirection of network traffic (also known as source port routing). We interviewed data telecommunication specialists and tested routers at one location. Only the CI routers were configured to deny source port routing. Adequate controls may not be in place on the remaining IRS routers.

Another access control involves user identity impersonation, known as IP spoofing. A crafty intruder can gain access to sensitive taxpayer data by posing as an authorized user. To do this, an intruder sends electronic information that appears to originate from inside the IRS' WAN. The IRS routers we tested use software that adequately prevents known IP spoofing attacks. To ensure continued success against these types of attacks, the IRS needs to ensure the most current software revisions are installed on its LAN routers.

Denial-of-Service

As the IRS continues to take advantage of the Internet, adequate controls need to be in place to make sure the IRS' applications and systems are always available for use by employees (Intranet) and taxpayers (Internet).

One of the most devastating attacks on a telecommunications system is the denial-of-service attack. With this type of attack, intruders attempt to disrupt regular computer system processes and operations by shutting down or flooding routers with irrelevant data. We found router configurations for some sites properly configured to recognize irrelevant data or computer information requests to reduce the effect of denial-of-service attacks. Others were not configured to recognize these attacks.

Without proper router controls in place, a denial-of-service attack could cause LAN congestion ultimately resulting in shutting down operations throughout the IRS' LAN/WAN. Additionally, attacks could disable e-mail, Internet browsing, and other LAN capabilities, such as a system shut down. Recently there have been several denial-of-service attacks against non-government entities.

Audit Trails of Router Traffic

Audit trails provide records of transactions that verify activity on an information system. The network router should log all pertinent information (an audit trail) about user identities and their originating location. In the event of router hardware or software failure, a log of all router traffic will be readily available.

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

CI Division routers log information to a centralized location in its National Operations Center. The data are reviewed daily for signs of unusual activity. However, based on interviews with data telecommunications specialists and tests at one location, adequate controls may not be in place on the remaining IRS routers.

At one location tested, the router configuration did not send information about router accesses to another information system. Consequently, information about router traffic was not captured to enable identification of inappropriate activity.

Security measures for transmitting data enable the IRS to protect its confidentiality. Adequate telecommunication design also provides a means for continued operations by preventing potential intruders from disrupting systems.

Recommendation

4. The CIO should develop and implement a strong security policy for the IRS' LAN telecommunications (router) configurations. The security policy should clearly define the roles and responsibilities for the IRS data telecommunication specialists and outside contractors who interact with

the IRS' LAN telecommunications (routers) configurations. The policy should also define which routers are covered, and assign responsibilities for the implementation and the maintenance of the policy.

Conclusion

Without adequate LAN security policies and controls, the IRS risks the following types of security breaches:

- Unauthorized access to LANs, systems and data.
- Loss or destruction of assets (hardware, software, data).
- Theft or misuse of assets (hardware, software, data).
- Loss of integrity, confidentiality and availability of systems.
- Introduction of undesirable software or programs.
- Interruptions in the continuity of operations and service.

The IRS should implement policies and controls to provide consistent LAN security measures throughout its operations. It also needs to complete development of its control structure, security guidelines and procedures for its LAN systems and applications. These measures can help prevent continued attempts from outsiders to break into LANs. These actions can also limit the effects of malicious acts by employees.

Implementation of our recommendations could reduce: 1) delays in processing and collecting taxes due to 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 policies and guidelines used to establish sufficient security for the Internal Revenue Service's (IRS) local area networks (LANs) and related telecommunication processes. To accomplish our objective, we:

- Analyzed the development and communication of the IRS' policies and guidelines, and 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 the following specific components of information systems security:

Operational Security - the effectiveness of controls over support activities for major information systems located at the IRS' facilities. The reviews considered the adequacy of policies and procedures available for systems administrators and users to implement LAN security measures.

Telecommunications Security - security controls over: 1) the IRS' LANs, including controls over network hardware and software, such as firewalls, routers, and local communications ports; and 2) access to the Treasury Communications System (TCS) from inside and outside the Treasury firewall. These reviews considered whether adequate controls were in place over:

- Operation and configuration of the selected systems and networks.
- Network hardware such as routers and local communications ports.

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

- Computing Center - 1
- Service Center - 1
- Service Center Posts-of-Duty -2
- Software Development Center - 1
- District Office Headquarters - 3
- District Office Posts-of-Duty (with computer room) - 3
- District Office Posts-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:

Operational Security

I. 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 Internal Revenue Manual

II. Analyzed and assessed the significance of differences between IRS procedures and industry/government standards.

III. Interviewed staff from the offices of the Chief Information Officer (CIO), Assistant Commissioner (AC)-Service Center Systems, AC-Computing Center Systems, Regional Directors of Information Systems (IS), and IS managers and staff at the IRS' facilities reviewed to identify and discuss policies and guidelines used to implement and maintain security for computing centers, service centers, and district/regional computer facilities.

IV. To determine the effect of any absence of development or communication of computer security policies and guidelines, we evaluated the effectiveness of physical security controls in computer facilities. To accomplish this we:

A. Reviewed local security procedures and interviewed responsible security managers to ascertain the adequacy of local physical security policies and procedures.

B. Reviewed local security procedures and interviewed responsible security managers to ascertain the adequacy of local logical access security policies and procedures.

C. Reviewed local security procedures and interviewed responsible security managers to determine whether the facility's systems currently in operation were certified with the following documentation:

1. Risk assessment.
2. Computer security plan.
3. Trusted Facility Manual.
4. User Guides.

D. Reviewed local security procedures and interviewed responsible security managers to ascertain the adequacy of local telecommunications security policies and procedures.

<u>Telecommunications Security</u>

V. To evaluate security controls over: 1) the IRS' networks, including security controls over network hardware and software, such as firewalls, routers, and communications ports; and 2) access to the TCS from inside and outside the Treasury firewall, we:

A. Evaluated the operation and configuration of the selected systems and networks by reviewing documentation and interviewing the system administrators to identify:

1. System hardware and configuration used, such as:

a) Name, version of the network, and vendor (IBM, Banyon, etc.), and network topology (star, bus, ring).

b) Types of network interface cards used (Ethernet, LocalTalk, etc.).

c) Number, type and capacities of file servers used.

d) Number and kinds of workstations.

e) Other types of hardware used on the network (fax machines, modems, scanners, plotters, etc.).

2. Systems software used, applications available, and data residing on the network, such as:

a) Network operating system (Novell NetWare, etc.) and version.

b) Workstation operating systems (DOS, OS/2, Windows, Windows/NT, etc.).

c) Network protocols (TCP/IP, etc.).

d) Type of error checking and error correcting software; and security packages or tool kits used to detect and deter network break-ins.

B. Evaluated operational controls over hardware and software by determining whether:

1. A centralized organization has provided guidance throughout the IRS and direction on approval and control of telecommunications equipment.

2. An individual(s) has been designated as responsible for the approval and control of telecommunications equipment.

C. Interviewed security officers to determine whether:

1. Any system hardware was physically damaged or accessed by unauthorized users.

2. Telecommunications software was altered or accessed by unauthorized users.

D. Determined whether the following controls were implemented to reduce the risks related to systems hardware:

1. Limited access to vulnerable areas such as wiring closets, patch panels, or encryption devices.

2. Use of cable types such as fiber optics, that are difficult to tap.

3. Restricted access to test equipment, such as data scopes or line monitors (hardware and software that analyzes traffic, detects bottlenecks and problems in a network).

E. Determined whether the following controls were implemented to reduce the risks related to telecommunications software:

1. Logging all program accesses and changes.

2. Defining telecommunications software resources (e.g., libraries, definition tables, etc.) to an access control facility and restricting access to only authorized user IDs.

VI. We evaluated the controls over network hardware such as routers, and local communications ports.

A. Determined whether adequate change controls were in place over network hardware configuration, and whether the configuration is periodically monitored. This included determining whether the system administrator:

1. Disabled all unnecessary communications ports for the systems attached to the network.

2. Regularly checked for resets done by the communications vendor.

3. Properly configured routers based on the following Tax Systems Modernization Institute (*TSMI*) CISCO router security tests:

    a) Restrict telnet access.

    b) Deny source port routing (redirecting traffic).

    c) Effectively log information on the syslog host.

    d) Reduce the effect of denial-of-service attacks.

4. Maintained hard copies (or other backups) of router configurations.

5. Maintained a documented plan for configuring routers and local communications ports to only permit access from authorized locations. (This included identification of potential risks such as address spoofing.)

B. Evaluated configuration controls over access to local networks through routers and local communications ports, and determined whether:

1. A centralized organization has provided effective guidance and direction throughout the IRS.

2. An individual(s) has been designated as responsible for making sure local network and router configurations provide the proper level of security.

C. Reviewed regional security incident reports to determine whether unauthorized individuals (hackers) have gained access to local networks by exploiting security weaknesses in router configurations.

D. Assessed whether strong logical controls were in place, such as passwords and encryption, whenever routers and local communication ports cannot be adequately configured.

Note: Specific audit objectives and review results about Treasury Inspector General for Tax Administration (TIGTA) control tests for physical and logical access security are included in the following separate TIGTA reports:

- “The Internal Revenue Service Can Improve Information Systems Physical Security”
- “The Internal Revenue Service Can Improve Software-Based Access Controls to Enhance Security for Local Area Networks”

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 D. Lessa, Senior Auditor
Bruce Polidori, Senior Auditor
Suzanne Noland, Auditor
William Tran, Auditor

Appendix III

Report Distribution List

Chief Information Officer IS
Director, Information Systems Field Operations IS:F
Deputy Chief Information Officer, Operations IS
Director, Service Center Operations IS:SC
Director, Office of Security and Privacy Oversight IS:SPO

Appendix IV

Glossary of Terms

Attack - A set of actions that result in denial or degradation of service or a compromise of information, integrity, authentication, nonrepudiation, or other security feature.

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

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

C2 Security Level – The National Computer Security Center is the arm of the United States (U.S.) National Security Agency that defines criteria for trusted computer products. Following are the Trusted Computer Systems Evaluation Criteria (TCSEC), the Department of Defense (DOD) Standard 5200.28 (also known as the Orange Book), and the European equivalent. The Red Book is the Orange Book counterpart for networks.

- Level D is a non-secure system.
- Level C provides discretionary access control. The owner of the data can determine who has access to it.
- C1 requires user log-on, but allows group ID.
- C2 requires individual user log-on with password and an audit mechanism.

Levels B and A provide mandatory access control. Access is based on standard DOD clearances. Each data structure contains a sensitivity level, such as top secret, secret and unclassified, and is available only to users with that level of clearance.

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.

Crack or Cracker - A person that breaks into a computer system without authorization, whose purpose is to do damage (destroy files, steal credit card numbers, plant viruses, etc.). See hacker.

Denial-of-Service Attacks - An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a denial-of-service attack interrupts network service for some period.

E-mail - The transmission of memos and messages over a network. Users can send mail to a single recipient or broadcast it to multiple users.

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.

Firewall - A method for keeping a network secure. It can be implemented in a single router that filters out unwanted packets, or it may use a combination of technologies in routers and hosts. Firewalls are widely used to give users access to the Internet in a secure fashion as well as to separate a company's public Web server from its internal network. They are also used to keep internal network segments secure. For example, a research or accounting subnet might be vulnerable to snooping from within.

Hacker - Traditionally, a person who enjoys learning details of a programming language or operating system through doing rather than simply theorizing. In common usage, though, "hacker" is synonymous with "cracker" (i.e., someone who breaks into someone else's computer system, often on a network). A cracker may do this for profit, malice, or because the challenge is there.

Internet - A near-global network of computers joined by high speed, digital telecommunications that use a common rule set known as TCP/IP.

Intranet - A network that is contained within an enterprise, usually consisting of many interlinked local area networks. The network may also use leased lines over a wide area network (WAN) and connections through gateways to the Internet.

Internet Protocol (IP) - A communications protocol developed under contract from the DOD to internetwork dissimilar systems. This de facto UNIX standard, which is the protocol of the Internet, is becoming the global standard for communications.

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.

Mainframe Computer - There are small, medium and large-scale mainframes, handling from a handful 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 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. As a result, 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.

Minicomputer - A medium-scale computer that functions as a multi-user system for up to several hundred users.

Modem - (MOdulator-DEModulator) A device that adapts a terminal or computer to a telephone line. It converts the computer's digital pulses into audio frequencies (analog) for the telephone system and converts the frequencies back into pulses at the receiving side. The modem also dials the line, answers the call and controls transmission speed.

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 Risk Assessment - A risk assessment is the process of identifying threats and vulnerabilities of information systems or applications and evaluating alternatives for mitigating or accepting the resulting appropriate judgements about system controls and risks. Risk assessments should occur throughout the life cycle. A qualitative method is preferred. The risk assessment should focus on the system application, but should consider any risks posed by the physical environment in which the system operates.

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, 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 Security - Operational 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.

Router - A device that forwards data packets from one LAN or WAN to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Routers work at layer 3 in the protocol stack, whereas bridges and switches work at the layer 2.

Routers are used to segment LANs in order to balance traffic within workgroups and to filter traffic for security purposes and policy management. Routers are also used at the edge of the network to connect remote offices.

Security Features User's Guide - A single summary, chapter, or manual in the user documentation shall describe the security features provided by the information, guidelines on how to use them, and how they interact with one another.

Security Plan - A security plan provides a summary of the security requirements of each sensitive system or application and the organization's plan for meeting those requirements.

Sensitive But Unclassified (SBU) Systems / Data - Any information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a Title 5, U.S. Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of the Congress to be kept secret in the interest of national defense or foreign policy.

Source Port Routing or Source Route Bridging - A communications protocol in which the sending station is aware of all the bridges in the network and predetermines the complete route to the destination station before transmitting.

System Administrator - A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system 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.

Telnet - A terminal emulation protocol commonly used on the Internet. It allows a user to log onto and run a program from a remote terminal or computer. Telnet was originally developed for ARPAnet and is part of the TCP/IP communications protocol.

TRW - Thompson, Ramos, Wooldridge Inc. is a global technology, manufacturing, and service company strategically focused on supplying advanced technology products and services to the automotive, space, defense and information systems markets.

Trusted Facility Manual - A manual addressed to the system administrator, operator, and Information Systems staff which presents cautions about functions and privileges that must be controlled when running a security facility. The manual shall also include the procedures for examining and maintaining the audit record structure for each audit event.

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

Wide Area Network (WAN) - A communications network that covers a wide geographic area, such as state or country.

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 that had the exposure.
- The 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 security exposures are presented in the following major categories:

- Operational Security.
- Telecommunications Security.

The table includes the following abbreviations:

DCU - Data-communications Utility

EP/EO - Employee Plans and Exempt Organizations

IRM - Internal Revenue Manual

IS:O:O - The IRS' Information Systems function's Office of National Operations, Telecommunications Division

OMB - Office of Management and Budget

TRW - Thompson, Ramos, Wooldridge Inc.

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION								REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	TRW / IS:O:O - DCU	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
OPERATIONAL SECURITY													
Information Systems does not have a security plan for telecommunication operations and has not completed a network risk assessment.	X	X	X		X								OMB Circular No. A-130 Treasury Directive P 71-10 Security Plan - IRM 2.1.10.2.6 Risk Assessment - IRM 2.1.10.8
Sites need to be sure information systems working on their routers meet Treasury Directives/IRS requirements for certification and accreditation.		X	X	X	X			X		X	X		IRM 2.1.10.2.3.1
The sites either did not have the Security Features User's Guide for sensitive but unclassified data (SBU), or their guides did not include all the required security elements.		X	X	X	X			X		X	X		IRM 2.1.10.1.4.13

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION								REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	TRW / IS:O:O - DCU	Support Services	Examination	Collection	Appeals	Criminal Investigation	EP/EO	
OPERATIONAL SECURITY													
We found no evidence of Trusted Facility Manuals being prepared for SBU.		X	X	X	X			X		X	X		Doc 9627 Chapter 5
TELECOMMUNICATIONS SECURITY													
Potential security weaknesses identified in router configurations. Controls are not in place to restrict access from outside the network, prevent redirection of network traffic, reduce the effect of denial-of-service attacks, and maintain system log audit trails.	X	X	X	X	X	X							Doc. 9627 Chapter 5
Telecommunication operational procedures do not exist for instances where encryption fails or needs to be turned off.			X	X	X	X							IRM 2.1.10.5.2

Appendix VI

Template: General Support System Security Plan[1]

SYSTEM IDENTIFICATION
Date:

System Name/Title

- Unique Identifier and Name given to the system.

Responsible Organization

- List organization responsible for the system.

Information Contact(s)

- Name of person(s) knowledgeable about, or the owner of, the system.

  Name
  Title
  Address
  Phone

Assignment of Security Responsibility

- Name of person responsible for security of the system.

  Name
  Title
  Address
  Phone

System Operational Status

If more than one status is selected, list which part of the system is covered under each status.

- Operational
- Under Development
- Undergoing a major modification

General Description/Purpose

- Describe the function or purpose of the system and the information processed.
- Describe the processing flow of the application from system input to system output.

[1] Source: NIST Special Publication 800-18, December 1998

- List user organizations (internal and external) and type of data and processing provided.
- List all applications supported by the general support system. Describe each application's functions and information processed.

System Environment

- Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)
- Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
- Include any security software protecting the system and information.

System Interconnection/Information Sharing

- List of interconnected systems and system identifiers (if appropriate).
- If connected to an external system not covered by a security plan, provide a short discussion of any security concerns that need to be considered for protection.
- It is required that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

Applicable Laws or Regulations Affecting the System

- List any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

General Description of Information Sensitivity

- Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: High, Medium, or Low.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

MANAGEMENT CONTROLS

Risk Assessment and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

Review of Security Controls

- List any independent security reviews conducted on the system in the last three years.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

Rules of Behavior

- A set of rules of behavior in writing must be established for each system. The rules of behavior should be made available to every user prior to receiving access to the system. It is recommended that the rules contain a signature page to acknowledge receipt.
- The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. They should state the consequences of inconsistent behavior or noncompliance. They should also include appropriate limits on interconnections to other systems.
- Attach the rules of behavior for the system as an appendix and reference the appendix number in this section or insert the rules into this section.

Planning for Security in the Life Cycle

- Determine which phase(s) of the life cycle the system or parts of the system are in. Describe how security has been handled in the life cycle phase(s) that the system is currently in.

Initiation Phase

- Reference the sensitivity assessment, which is described in Section 3.7 of Special Publication 800-18, *Sensitivity of Information Handled*.

Development/Acquisition Phase

- During the system design, were security requirements identified?
- Were the appropriate security controls with associated evaluation and test procedures developed before the procurement action?
- Did the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- If this is a purchased commercial application or the application contains commercial, off-the-shelf components, were security requirements identified and included in the acquisition specifications?

Implementation Phase

- Were design reviews and systems tests run prior to placing the system in production? Were the tests documented? Has the system been certified?
- Have security controls been added since development?
- Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?
- Include the date of the certification and accreditation. If the system is not authorized yet, include date when accreditation request will be made.

Operation/Maintenance Phase

- The security plan documents the security activities required in this phase.

Disposal Phase

- Describe in this section how information is moved to another system, archived, discarded, or destroyed. Discuss controls used to ensure the confidentiality of the information.
- Is sensitive data encrypted?
- How is information cleared and purged from the system?
- Is information or media purged, overwritten, degaussed or destroyed?

Authorize Processing

- Provide the date of authorization, name, and title of management official authorizing processing in the system.
- If not authorized, provide the name and title of manager requesting approval to operate and date of request.

OPERATIONAL CONTROLS

Personnel Security

- Have all positions been reviewed for sensitivity level?
- Have individuals received background screenings appropriate for the position to which they are assigned?
- Is user access restricted to the minimum necessary to perform the job?
- Is there a process for requesting, establishing, issuing, and closing user accounts?
- Are critical functions divided among different individuals (separation of duties)?
- What mechanisms are in place for holding users responsible for their actions?
- What are the friendly and unfriendly termination procedures?

Physical and Environmental Protection

- Discuss the physical protection for the system. Describe the area where processing takes place (e.g., locks on terminals, physical barriers around the building and processing area, etc.).
- Factors to address include physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems.

Production, Input/Output Controls

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, software should be listed. In this section, provide a synopsis of the procedures in place that support the system. Below is a sampling of topics that should be reported in this section.

- User support - Is there a help desk or group that offers advice?
- Procedures to ensure unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Audit trails for receipt of sensitive inputs/outputs.
- Procedures for restricting access to output products.
- Procedures and controls used for transporting or mailing media or printed output.
- Internal/external labeling for sensitivity (e.g., Privacy Act, Proprietary).
- External labeling with special handling instructions (e.g., log/inventory. identifiers, controlled access, special storage instructions, release or destruction dates).
- Audit trails for inventory management.
- Media storage vault or library-physical, environmental protection controls/procedures.

- Procedures for sanitizing electronic media for reuse (e.g., overwriting or degaussing).
- Procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse.
- Procedures for shredding or other destructive measures for hardcopy media when no longer required.

Contingency Planning

Briefly describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster were to occur. If a formal contingency plan has been completed, reference the plan. A copy of the contingency plan can be attached as an appendix.

- Any agreements of backup processing.
- Documented backup procedures including frequency (daily, weekly, monthly) and scope (full, incremental, and differential backup).
- Location of stored backups and generations of backups kept.
- Are tested contingency/disaster recovery plans in place? How often are they tested?
- Are all employees trained in their roles and responsibilities relative to the emergency, disaster, and contingency plans?

Hardware and System Software Maintenance Controls

- Restriction/controls on those who perform maintenance and repair activities.
- Special procedures for performance of emergency repair and maintenance.
- Procedures used for items serviced through on-site and off-site maintenance (e.g., escort of maintenance personnel, sanitization of devices removed from the site).
- Procedures used for controlling remote maintenance services where diagnostic procedures or maintenance is performed through telecommunications arrangements.
- Version control that allows association of system components to the appropriate system version.
- Procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production.
- Impact analyses to determine the effect of proposed changes on existing security controls to include the required training for both technical and user communities associated with the change in hardware/software.
- Change identification, approval, and documentation procedures.
- Procedures for ensuring contingency plans and other associated documentation are updated to reflect system changes.
- Are test data “live” data or made-up data?
- Are there organizational policies against illegal use of copyrighted software or shareware?

Integrity Controls

- Is virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?
- Are reconciliation routines used by the system, i.e., checksums, hash totals, record counts? Include a description of the actions taken to resolve any discrepancies.
- Are password crackers/checkers used?
- Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions?
- Are intrusion detection tools installed on the system?
- Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?
- Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately?
- Is message authentication used in the system to ensure that the sender of a message is known and that the message has not been altered during transmission?

Documentation

Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information systems security of the system to include backup and contingency activities, as well as descriptions of user and operator procedures.

- List the documentation maintained for the system (vendor documentation of hardware/software, functional requirements, security plan, program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, authorization for processing, verification reviews/site inspections).

Security Awareness & Training

- The awareness program for the system (posters, booklets, and trinkets).
- Type and frequency of general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training).
- The procedures for assuring that employees and contractor personnel have been provided adequate training.

Incident Response Capability

- Are there procedures for reporting incidents handled either by system personnel or externally?
- Are there procedures for recognizing and handling incidents, (i.e., what files and logs should be kept, who to contact, and when)?

- Who receives and responds to alerts/advisories, (e.g., vendor patches, exploited vulnerabilities)?
- What preventative measures are in place, (i.e., intrusion detection tools, automated audit logs, penetration testing)?

TECHNICAL CONTROLS

Identification and Authentication

- Describe the method of user authentication (password, token, and biometrics).
- If a password system is used, provide the following specific information:
  - Allowable character set.
  - Password length (minimum, maximum).
  - Password aging time frames and enforcement approach.
  - Number of generations of expired passwords disallowed for use.
  - Procedures for password changes.
  - Procedures for handling lost passwords.
  - Procedures for handling password compromise.
- Procedures for training users and the materials covered.
- Indicate the frequency of password changes, describe how password changes are enforced (e.g., by the software or System Administrator), and identify who changes the passwords (the user, the system, or the System Administrator).
- Describe any biometrics controls used. Include a description of how the biometrics controls are implemented on the system.
- Describe any token controls used on this system and how they are implemented.
- Describe the level of enforcement of the access control mechanism (network, operating system, and application).
- Describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual).
- Describe the self-protection techniques for the user authentication mechanism (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text passwords, passwords are automatically generated, passwords are checked against a dictionary of disallowed passwords).
- State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.

- Describe the procedures for limiting access scripts with embedded passwords (e.g., scripts with embedded passwords are prohibited, scripts with embedded passwords are only allowed for batch applications).
- Describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies (e.g., host-to-host, authentication servers, user-to-host identifier, and group user identifiers) and any compensating controls.
- If digital signatures are used, the technology must conforms to FIPS 186, Digital Signature Standard and FIPS 180-1, Secure Hash Standard issued by NIST, unless a waiver has been granted. Describe any use of digital or electronic signatures.

Logical Access Controls

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists (ACLs).
- How are access rights granted? Are privileges granted based on job function?
- Describe the system's capability to establish an ACL or register.
- Describe how users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent user from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

Audit Trails

- Does the audit trail support accountability by providing a trace of user actions?
- Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection?
- Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)

- Is access to online audit logs strictly enforced?
- Is the confidentiality of audit trail information protected if, for example, it records personal information about users?
- Describe how frequently audit trails are reviewed and whether there are guidelines.
- Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem?