The Internal Revenue Service Can Improve Information Systems Physical Security

February 2000

Reference Number: 2000-20-039

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

February 15, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Can Improve Information Systems Physical Security

This report presents the results of our reviews to assess the adequacy of the Internal Revenue Service's (IRS) physical security for its information systems. 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 logical access security, which will be reported on separately.

In summary, the IRS has taken considerable steps to improve its security program. However, assessing and reducing risks at over 1,000 IRS facilities is a significant undertaking. In implementing its security program, the IRS needs to consistently apply physical security standards throughout its organizational components. Specifically, the IRS can improve physical security controls over information systems in the following areas: access controls, fire protection, environmental controls, and magnetic media management.

To address these conditions we recommended that the Chief Information Officer, in conjunction with other IRS executives, take steps to address the specific weaknesses identified in this report and to ensure that minimum physical security standards are met in all offices. These steps also include prioritizing the weaknesses and obtaining funds to correct them.

Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

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

Physical security is the most fundamental form of information systems control. Physical security controls are implemented to protect sensitive areas housing information systems equipment or data. Sensitive areas requiring physical controls include computer rooms, communication wire closets, and areas housing essential support equipment, such as power control panels, air conditioning units, communication equipment, and magnetic media storage. Physical security controls protect information systems hardware, software, and data from theft, physical damage, unauthorized disclosure, and interruption of service.

The overall objective of this review was to assess the adequacy of physical security controls over the Internal Revenue Service's (IRS) information systems and sensitive data. 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 logical access security, which will be reported separately.

Results

The IRS has taken considerable steps to improve its security program. However, assessing and reducing risks at over 1,000 IRS facilities is a significant undertaking. We found that the IRS does not consistently apply physical security standards throughout all of its organizational components. By using prescribed controls, the IRS can reduce information systems physical security weaknesses in the following four areas:

- Access controls: Construction of computer rooms and related facilities did not always meet the IRS and United States Treasury requirements for minimum security. Controls restricting the entry and exit of personnel, equipment, and magnetic media were not always in place in areas such as computer rooms, tape libraries, or rooms containing local area network file servers.
- Fire protection: Adequate fire extinguishing and evacuation instructions were not always posted in strategic locations, computer room fire detection systems did not always include properly placed smoke and heat detection devices or fire alarm pull

boxes, and all automatic fire extinguishing systems were not appropriate for computer rooms.

- Environmental controls: Preventive maintenance, cleaning, and inspection of computer equipment and facilities was not always performed; thermometers and humidity indicators to identify unsuitable temperature and humidity levels were not always turned on and monitored; and computer rooms and related facilities were not always protected from potential water damage.
- Magnetic media management: Management of the magnetic media inventory did not always ensure accountability and accessibility of disks and tapes to operate the IRS' information systems.

Addressing these weaknesses will improve information systems security. Both the level of risk and the severity of the exposure should be considered in taking actions to improve information systems security.

Summary of Recommendations

The Chief Information Officer (CIO), in conjunction with other IRS executives, should identify physical security weaknesses and take steps to address them. These steps will require IRS management to assess the state of physical security and prioritize the need to address identified weaknesses. These steps include seeking and obtaining funds to correct the conditions that require attention. The CIO can use the Office of Security Standards and Evaluation to evaluate the progress the IRS has made in meeting plans to eliminate or reduce the identified weaknesses.

Management's Response: The IRS' Office of Security and Privacy Oversight has designated its Director of the Office of Security Evaluations and Oversight to work in conjunction with other IRS executives to establish minimum physical security requirements for information systems operations at all IRS facilities.

The Office of Security Evaluations and Oversight currently performs about 150 reviews at various facilities each year. This office is acquiring contractor support to help with its effort. These security efforts will not focus on visiting the over 1,000 IRS facilities in the short term. Instead, the IRS will continue to work issues in a facility-type approach. This approach intends to initiate facility-wide improvements.

As part of these reviews, the Office of Security Evaluations and Oversight conducts follow-up reviews to assess the progress that sites make to reduce identified risks. It also conducts problem-solving visits to work with local staff to develop corrective actions for unresolved risks.

The IRS is also making a large financial commitment to maintain its efforts. It continues to work with the Department of the Treasury and its bureaus to obtain additional security funds for critical infrastructure protection. To date, however, the IRS has not identified any additional funding sources.

Objective and Scope

The overall objective of this review was to assess the adequacy of physical security controls over the Internal Revenue Service's (IRS) information systems and sensitive data. The review considered whether:

1. Program goals are adequately defined, communicated, implemented, and maintained.
2. Program assets (including data) are adequately safeguarded.

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

We visited 24 IRS sites between March and May 1999. The IRS facilities we visited had varying operations and geographical make-up. We performed these reviews in accordance with *Government Auditing Standards* in the following facilities: computing center, service center, service center posts of duty, software development center, district office headquarters, and district office posts of duty. Review steps included identifying and analyzing the IRS security control structure and existing physical security procedures. We also made assessments of the physical security measures in place at the sites visited.

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

Adequate physical security can help prevent:

- *Interruptions in computer services.*
- *Physical damage.*
- *Unauthorized disclosure of information.*
- *Loss of control over system integrity.*
- *Theft.*

The purpose of computer information systems 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.

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

The IRS has a very large and diverse network of computer systems that it uses to process over 200 million tax returns and collect $1.7 trillion in taxes annually. It operates over 1,000 facilities (computing centers, service centers, and regional, district, and outlying offices) that support tax processing.

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' 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 its facilities, serious weaknesses persist.

The Congress recognized the significance of maintaining adequate information systems security in the IRS Restructuring and Reform Act of 1998 (RRA 98).[1] This law directs the newly established Office of 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 security practices. The IRS has taken considerable steps to improve its security program. These steps include the creation of the Office of Security Standards and Evaluation (SSE). In 1998, the SSE began performing security risk assessments at the IRS' facilities nationwide. In addition to the risk assessments, the SSE is working with IRS management to correct 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 information systems security, the IRS' organizational components do not consistently apply physical security standards throughout all facilities. Specifically, the IRS can improve physical security over information systems in the following four areas:

- Access controls
- Fire protection
- Environmental controls
- Magnetic media management

[1] Internal Revenue Service Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685 (1998)

By addressing these weaknesses the IRS will reduce the effects of exposures to its information systems security. Eliminating or reducing these exposures involves assessing and managing available resources to address potential security threats. The level of risk associated with the severity of the exposure can direct the IRS in taking actions to improve information systems security.

By Consistently Applying Security Standards, the Internal Revenue Service Can Improve Physical Security

All IRS organizational components need to follow IRM guidance to ensure information systems operations meet minimum security requirements.

The Internal Revenue Manual (IRM) provides guidance on information systems security policies and procedures. Parts 1 and 2 of the IRM comprehensively cover minimum security standards. Although these IRM sections are available nationwide, all of the IRS' organizational components did not consistently and comprehensively apply the minimum security standards in the facilities reviewed.

Several organizational components are responsible for security over the IRS' information systems.

- Information Systems (IS) has responsibility for security over district telecommunications equipment and the Examination and Collection Divisions' file servers and computer workstations.
- Criminal Investigation, Appeals, and the IRS Chief Counsel each control the security over their own file servers and computer workstations.
- Support Services manages physical security over existing building components, initial construction, and space occupation.

These functions applied varying emphasis on, and interpretation of, the minimum standards for information systems security. Differences in application of the security standards existed among functions as well as within functions in different locations.

Management decisions for meeting security requirements varied by their understanding and interpretation of the IRM guidance or their attempt to access funding.

In some instances, management at the facilities:

- Did not recognize the requirement to implement some of the minimum security measures.
- Recognized the requirement for security measures but chose not to implement them.
- Recognized the need for the security measures but did not seek the funds to meet the minimum security requirements.

In one instance, the IRS planned and constructed a new district office facility. Support Services designed the construction of the computer room using the IRS' requirements for an "equipment room." This design did not meet the minimum requirements for computer room operations as prescribed in the IRM. The controls that are required for computer rooms but not equipment rooms include slab-to-slab wall construction, a fire detection system, deadbolt locks, secure hinges, and drainage. The equipment room controls were not sufficient to protect the district's information systems equipment and data from theft, alteration, or damage from unauthorized access, fire, or environmental problems.

IRS management's reasons for the constructed design were cost considerations and an absence of a complete understanding of the purpose of the minimum physical security requirements for a computer room.

In another instance, a district office was not aware of basic controls, such as restricted access to the tape library and proper routing of water pipelines. Although these controls are detailed in the IRM, neither the district IS function security analyst nor the Support Services branch chief had knowledge of the current requirements.

Compliance with policies, procedures, and guidelines by the IRS' organizational components can help:

- Sustain operations.

Physical security exposures exist in the IRS' information systems as a result of noncompliance with established guidelines.

- Account for, protect, and optimize the IRS' use of available information systems hardware.
- Maintain current systems and plan and model future systems.
- Provide administrators and users an adequate understanding of security requirements to help ensure the integrity of the systems and data.

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

Specifically, the IRS needs to address the following issues to meet minimum physical security standards.

Access Controls Issues

Physical access controls restrict the entry and exit of personnel, equipment, and magnetic media. These controls restrict access to areas such as computer rooms, tape libraries, or rooms containing local area network file servers.

The IRS needs to consistently implement the following physical access controls over information systems facilities:

Physical access security is the ability to grant selective physical access to specific personnel at certain times and deny access to all other personnel at all times.

- Proper construction of doors (including appropriate signs), locks, hinges, and walls will improve security over access to computer facilities. Information systems equipment, including file servers, should be located in areas where access is restricted.
- Computer room entrance logs should be used by all persons without card key access and should include dates and times of all persons entering the facility. If a questionable event requires identifying the potential participants involved, records of presence in the computer room allow for accountability of personnel.
- Adequate control and accounting of entrance cards, keys, and door combinations will help ensure only

appropriate personnel access computer facilities. Also, only personnel with a need to access the facility should have entrance cards, keys, or combinations (keys should not be on the facility-wide key access system, i.e., "master key system"). Unused equipment should be removed from computer rooms to further reduce a need for access.

Consistent implementation of controls over physical access to computer rooms and supporting facilities will allow the IRS to meet minimum physical security requirements by restricting access to only authorized staff with an official business need.

Fire Protection Issues

Fire, along with the resultant damage caused by fire extinguishing procedures, is one of the most common causes of damage to information systems equipment and data. The IRS needs to consistently implement the following fire protection measures for information system facilities:

It is important to evaluate the fire safety of buildings that house information systems. Smoke, corrosive gases, and high humidity from a localized fire can damage information systems throughout an entire building.

- Clear and adequate fire extinguishing and evacuation instructions should be posted in strategic locations to assist personnel in the event of a fire.
- Computer room fire detection systems should include properly placed smoke and heat detection devices. Fire alarm pull boxes should be appropriately placed.
- Computer room automatic fire extinguishing systems should be modified to dry pipe systems (sprinkler system water pipelines that do not hold standing water) and should be tested periodically by the manufacturer or service representative.

Adhering to fire protection requirements will help ensure the safety of employees, information systems, and data. Following these requirements will also promote continuity of operations and service.

Environmental Controls Issues

Environmental hazards to information systems include floods, water leaks, humidity, extreme temperatures, power failures, insufficient ventilation, and excessive dust or dirt. The IRS needs to consistently implement the following environmental controls to prevent interruptions of service:

Failures of electric power, heating and air conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware.

- Preventive maintenance, cleaning, and inspection of computer equipment and facilities should be performed routinely. Documentation of these actions should also be maintained.
- Thermometers and humidity indicators should be installed and monitored to identify unsuitable temperature and humidity levels. A trained person should monitor these instruments on a routine basis. Also, the temperature range of communication wire closets (also called Intermediate Distribution Facilities) should be the same as the adjacent office space at all times.
- Computer rooms should be constructed to prevent water damage. Overhead water and steam pipes should not be present, waterproof protective covers for computer equipment should be readily accessible, and computer room drainage should be sufficient to protect the entire room.

Adhering to environmental control requirements will help promote continuity of operations and service.

Magnetic Media Management Issues

Information systems capture electronic data on magnetically charged disks and tape, commonly referred to as magnetic media. Effective media management ensures accountability and accessibility of disks and tapes to operate the IRS' information systems. Back-up media are critical to continue operations in situations ranging from a minor loss of information to a disaster recovery predicament. The facility needs the back-up media from off-site storage to resume operations.

Without proper media protection, critical information could be lost and recovery time would significantly increase. In addition, the back-up media may contain sensitive taxpayer data, which, if not controlled, could be compromised.

Following its own procedures would help the IRS ensure efficient and effective magnetic media management.

The IRM includes procedures for managing magnetic media through several Tape Management Systems and for conducting tape inventory validations. The inventory process includes reporting inventory results to the IRS National Office Field Systems and Support Branch. This process includes reconciling and resolving inventory discrepancies and performing vulnerability studies for missing tapes.

To meet their prescribed procedures, management needs to ensure the following controls are consistently implemented.

- The magnetic media inventory should properly account for all tapes in libraries. Inventory systems varied from an absence of a system to ineffectively or improperly managed systems.
- Access to the tape libraries should be restricted to only those with a need for access. Access to the tape library was not always restricted; therefore, anyone with access to the area had access to the tapes. Access to the tape library should be restricted to prevent unauthorized access to taxpayer information.
- All back-up media should be accounted for and properly stored. Specifically, back-up tapes were not properly secured in all locations reviewed. Some locations did not send the back-up tapes to off-site storage. And, in one location, the off-site facilities' environmental conditions did not ensure adequate tape protection.

Management should follow prescribed procedures for accounting for and storing magnetic media, including back-up tapes.

- Back-up tapes should be created at planned times. At one location reviewed, IS management did not always ensure that they created back-up tapes for all systems. Also, back-up media should be scheduled for disposition and replacement to reduce the potential of data errors due to decay of the media.

By not tracking the tapes' age, offices cannot plan for disposition and replacement of the back-up tapes. As a result, offices may encounter data retrieval failure because the aged tape no longer works.

With the proper controls in place, magnetic media back-up information will be available when needed, and the information stored on the media will be safeguarded against unauthorized disclosure.

Recommendations

The Chief Information Officer, in conjunction with other IRS executives and field managers, should ensure that minimum physical security requirements for information systems operations are met in the IRS' facilities.

1. The executives need to take steps to address the specific weaknesses identified in this report. They also should perform reviews in all IRS locations to assess the state of physical security and take steps to reduce similar exposures in those locations. This will require IRS management to prioritize the need to reduce these exposures, including seeking and obtaining funds to correct the weaknesses.

   In performing these reviews and prioritizing the corrective actions necessary to address security weaknesses, IRS management needs to consider the risks and assume responsibility if they do not take corrective actions. To implement these activities, we suggest that:

– The IS, Support Services, and Compliance functions use existing guidelines and controls to review the state of physical security in their facilities and implement their respective requirements for physical access, fire protection, and environmental controls.

– The IRS' organizational components follow existing procedures for properly storing magnetic media and for conducting tape inventory validations. (The inventory process includes reporting inventory results to the IRS National Office Field Systems and

Support Branch. This process includes reconciling and resolving inventory discrepancies and performing vulnerability studies for missing tapes.)

Management's Response: The IRS' Office of Security and Privacy Oversight has designated its Director of the Office of Security Evaluations and Oversight to work in conjunction with other IRS executives to establish minimum physical security requirements for information systems operations at all IRS facilities.

The Office of Security Evaluations and Oversight currently performs about 150 reviews at various facilities each year. This office is acquiring contractor support to help with its effort. These security efforts will not focus on visiting the over 1,000 IRS facilities in the short term. Instead, the IRS will work issues in a facility-type approach. This approach intends to initiate facility-wide improvements.

The IRS is also making a large financial commitment to maintain its efforts. It is working with the Department of the Treasury and its bureaus to obtain additional security funds for critical infrastructure protection. To date, however, the IRS has not identified any additional funding sources.

2. The executives need to use the SSE to evaluate the progress the IRS has made in meeting plans to reduce or eliminate the identified exposures.

Management's Response: The Office of Security Evaluations and Oversight currently performs about 150 reviews at various facilities each year. As part of these reviews, it conducts follow-up reviews to assess the progress that sites make to reduce identified risks. It also conducts problem-solving visits to work with local staff to develop corrective actions for unresolved risks.

Conclusion

The IRS should implement policies and controls to provide consistent security measures throughout its operations. Without adequate physical control safeguards, the IRS risks security breaches, such as:

Practical computer security is a series of actions and counteractions of attacks and defenses.

- Loss or destruction of assets (hardware, software, and data).
- Theft or misuse of assets (hardware, software, and data).
- Introduction of undesirable software or programs.
- Interruptions in the continuity of operations and service.

Vigilance in implementing and maintaining this security program will help ensure the IRS meets 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; 2) opportunities to 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 physical security safeguards used to assure sufficient security for the Internal Revenue Service's (IRS) information systems and sensitive data. To accomplish our objective, we:

- Analyzed the development and communication of IRS policies and guidelines related to physical security.
- Reviewed the IRS' information systems oversight of physical security, including reviews performed by the Office of Security Standards and Evaluation.
- Performed tests and observations of physical security controls in the IRS facilities identified below.

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 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 - Management of Federal Information Resources.
- 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. To determine the effect of the 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. Evaluated controls in place to reduce the potential for the damage or theft of data and equipment and determined if existing physical security policies and procedures were adequate.

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

1. Ascertained whether the Information Systems function maintained a catalogue of current information systems policies and procedures (or equivalent) including whether there were documented written procedures in effect to prevent unauthorized persons from gaining access to computer facilities.
2. Obtained site maps, interviewed local security managers, and toured sites to locate and observe all computer-related facilities in the sites, including computer rooms, telecommunications closets, and utilities access points, and evaluated the adequacy of local physical security controls in use.
3. Interviewed security managers and reviewed local procedures to evaluate the adequacy of fire protection systems.
4. Determined whether environmental equipment was adequate to protect computer hardware from damage.

5. Reviewed back-up power supply documentation to determine if it had been tested and met criteria to be of adequate size to power-up critical systems and resume operations of: computer systems, emergency back-up lights, and any other relevant equipment or facilities.
6. Interviewed local security managers, obtained and reviewed local procedures, and observed tape library area to evaluate security controls over managing tape libraries.

C. Obtained and reviewed local data back-up procedures, interviewed security managers, and observed data back-up storage facilities. Evaluated the controls implemented to ensure data file back-up procedures effectively protected and prevented the loss of data.

D. Interviewed security managers, reviewed local application control procedures, and obtained local inventories/listings of both authorized and installed applications to evaluate application controls.

E. Obtained local security incident handling procedures and interviewed security managers to determine whether controls had been implemented to effectively identify and respond to security-related incidents.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Scott A. Macfarlane, Director
Stephen Mullins, Director
Edward Neuwirth, Audit Manager
Eulala Davis, Senior Auditor
Glen Rhoades, Senior Auditor
Michael Garcia, Auditor
Beverly Tamanaha, Auditor
Louis Zullo, Auditor

Appendix III

Report Distribution List

Deputy Commissioner Operations C:DO
Chief Information Officer IS
Chief Management and Finance M
Chief Operations Officer OP
Assistant Commissioner (Criminal Investigation) OP:CI
Assistant Commissioner (Information Systems Field Operations) IS:FO
Assistant Commissioner (National Operations) IS:O
Assistant Commissioner (Service Center Operations) IS:SC
Security Standards and Evaluation Office IS:E
National Director for Legislative Affairs CL:LA

Appendix IV

Glossary of Terms

Cipher Lock - A combination door lock used to restrict access.

Dry Pipe System - A sprinkler system employing automatic sprinklers attached to a piping system containing air or nitrogen under pressure, the release of which (from the open sprinklers) permits the water pressure to open a valve known as a dry pipe valve. The water then flows into the piping system and out the opened sprinklers.

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.

Intermediate Distribution Facility (IDF) - A telecommunications closet set aside for housing telecommunications equipment, cable and fiber terminations, and related cross-connections.

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.

Magnetic Media - Magnetically charged disks and tapes on which information systems data is captured and stored.

Main Distribution Facility (MDF) - An equipment room in a centralized space which houses communications (voice and data) common equipment, serving the occupants of the space.

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.

Operational and Physical Security - Operational security and physical security include established control structures that effectively manage and protect the integrity, confidentiality, and availability of information systems data and resources.

Restricted Access - Access is restricted to those persons who, due to their official duties and/or responsibilities, have a need for such access.

Secure Hinges - A door hinge modified with a pin to prevent removal.

Telecommunications 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 either by direct connections (i.e., via terminals) or indirect connections.

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
- 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 table includes the following abbreviations:

IRM - Internal Revenue Manual
TD - Treasury Directive
POD - Post of Duty
IDF - Intermediate Distribution Facility
NIST - National Institute of Standards and Technology
MDF - Main Distribution Facility
IIA - Institute of Internal Auditors' guidelines for Systems Auditability and Control
Doc 9399 - Information Systems Operations and Support Procedures

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Access to Facility:											
Deadbolts were not installed for use during non-duty hours.			X	X	X	X					TD P 71-10, VI-6.B.3
Hinges were located on the outside of the entrance and were not modified to preclude removal.			X	X	X	X					TD P 71-10, VI-6.B.3
The computer room or IDF walls were not slab-to-slab.	X		X	X	X	X					TD P 71-10, VI-6.B.3
The computer room entrance log was not used regularly and properly controlled for personnel who did not have card key access.			X	X	X						IRM 1.16.8.2.7.0 (2)a & TD P 71-10, VI-6.B.3

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Access to Facility:											
Entrances to IDFs were not locked when they were not in use.				X	X	X				X	IRM 1.16.8. 2.7.0 (2)c & TD P 71-10, VI-6.B.3
Entrance cards/keys/combos were not properly controlled and accounted for. Computer room/IDF locks were accessible by master keys.	X	X	X	X	X	X					IRM 1.16.8.4.9.4 (1), (9)a & TD P 71-10, VI-6.B.3
Entrance cards/keys/combos were not restricted to only those with a need to access the facility.			X	X	X	X					IRM 1.16.8.4.9.4 (1), (11) & TD P 71-10, VI-6.B.3

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Access to Facility:											
Access to computer rooms was not monitored to determine levels of usage and continuing need for access.			X	X	X	X					TD P 71-10, VI-6.B.3
Equipment not in use was warehoused in the computer room or IDF.	X		X	X	X	X	X				IRM 1.16.8.1.6.0
The access card system does not provide a listing of employees with a need for computer room/tape library access; the manual list was not kept current.			X		X	X					TD P 71-10, VI-6.B.3

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Access to Facility:											
The cipher lock to the IDF does not use at least four numbers.				X		X					TD P 71-10, VI-6.B.3
POD IDF keys were not restricted to only those with a need to access the facility.			X		X						IRM 1.16.8.4.9.4 (1), (11) & TD P 71-10, VI-6.B.3
The file servers and communications equipment were located in open workspace where access cannot be restricted.			X	X	X	X		X	X	X	IRM 2.1.10. 4.6(12)

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Access to Facility:											
The entrances to communication equipment rooms were labeled.			X	X	X	X					Consolidated Physical Standards for IRS Facilities pg. III - 37
Fire Protection:											
Clear and adequate fire instructions were not posted in strategic locations.	X	X	X	X	X	X					IRM 1(16)23 Sub.622 (1)(a), (2) & (3)
There were no smoke or heat detectors in the computer room.			X			X					IRM 2.1.7.2.5.2 & 2.1.10.6.7.1; NIST 3.10

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Fire Protection:											
There were no smoke detectors above the suspended ceiling in the computer room.	X	X	X	X	X	X					IRM 1.16.8.2.10.0 (3)k, & 1(16)41 Sub. 252 (2)(k)
Computer room/MDF did not have pull boxes to activate fire alarms.	X	X				X					IRM 1(16)41 Sub. 252 (2)(b)
The computer room fire extinguishing system was not periodically tested.				X		X					IIA 9-28

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Fire Protection:											
The sprinkler system in the computer room was not a dry pipe system.			X		X	X					IRM 2.1.10. 4.6(10); Western Region Voice & Data Com-munications 6/16/98 p.4; IIA 9-26
Waterproof protective covers for computer equipment were not available.	X	X	X	X	X	X					IRM 1(16) 23 Sub. 622 (1)(b) & 1.16.8. 2.10.0 (3)j

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Environmental Controls:											
The computer rooms and IDFs were not kept clean.			X	X	X	X					IRM 2.1.7.2.5.1
The computer room and MDF humidity alarms were not activated.	X	X			X	X					IRM 2.1.7.2.5.2 & 1.16.8 Section 2.10.0 (3)o
Thermometers and humidity indicators were not monitored on a routine basis.				X	X	X					IRM 2.1.7.2.5.2(1); Western Region Voice & Data Com-munications 6/16/98 p.3

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Environmental Controls:											
There was no drainage system in the computer room.			X	X	X	X					IRM 1(16)41 Sub. 252(2)(k)
The temperature range of IDFs was not the same as the adjacent office space.			X	X	X	X					Western Region Voice & Data Communications 6/16/98 p.3
The computer equipment was not subject to preventive maintenance, cleaning, and inspection.				X	X						IIA 4-36
Hazardous utilities (overhead water pipes) were present.				X		X					IIA 9-26

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Magnetic Media Management:											
Managers did not ensure that all media were properly stored.		X	X	X	X			X	X	X	IRM 2.1.10.6.8.2.2
Access to the tape library was not restricted.			X	X	X						IRM 1.16.8.2.10.5
Managers did not ensure that all magnetic media were accounted for.	X		X	X	X						IRM 2.1.10.6.8.2.2
Back-up tapes were not run at planned times.				X	X						IRM 2.1.10.6.8.2.2 (1)

SECURITY EXPOSURE	IRS FACILITY				RESPONSIBLE FUNCTION						REFERENCE
	Computing Center	Service Center	District Office	Post of Duty	Information Systems	Support Services	Examination	Collection	Appeals	Criminal Investigation	
PHYSICAL SECURITY											
Magnetic Media Management:											
The magnetic media inventory system does not properly account for tapes returned from back-up storage facilities.	X				X						IRM 2.1.8.4.2.1 (1); Doc. 9399 pg. 15 & 17
Environmental controls at the back-up storage facility were not adequate.			X			X					IRM 2.1.8.6.4 (4) & (5)
Back-up media were not scheduled for disposition and replacement to reduce the potential of data errors due to degradation.			X	X	X						Doc. 9399 pg. 25

Appendix VI

Management's Response to the Draft Report

COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

December 23, 1999

MEMORANDUM TO THE DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Charles O. Rossotti Coe
Commissioner of Internal Revenue

SUBJECT: Draft Audit Report – The Internal Revenue Service Can Improve Information Systems Physical Security

Thank you for the opportunity to review your draft report on physical security. We agree with its findings and recommendations, which we are currently addressing. As you know, the Internal Revenue Service (IRS) initiated an aggressive security management program in January 1997, when it established its Office of Systems Standards and Evaluation. Now called the Office of Security and Privacy Oversight (SPO), this Office's responsibilities include establishing and enforcing standards and policies for all major IRS security programs including, but not limited to, physical security, data security, systems security, and personnel security.

In August 1997, the IRS issued a "Limited Official Use" improvement plan in response to an earlier General Accounting Office (GAO) recommendation. The plan focuses on a facility-type approach, which is being used to more effectively mitigate weaknesses by (1) prioritizing and performing in-depth security evaluations and (2) working with upper management and the management of the facilities and support functions to prioritize and implement corrective actions. The actions being taken to implement the approach are consistent with GAO's suggestions for all federal agencies.

In this regard, the GAO recently reported that although a number of factors have contributed to weak federal information security—such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures—the fundamental underlying problem has been poor security program management. While the GAO identified a number of agencies that are affected by this problem, it noted that the IRS is one agency that has demonstrated the value of good management practices in strengthening security. Specifically, it noted that the IRS has made significant progress by acknowledging the seriousness of its computer security weaknesses, consolidating overall responsibility for computer security management, reevaluating its approach to computer security management, and developing an effective plan for mitigating weaknesses.

The GAO has also been the impetus for senior executives from other federal agencies meeting with the IRS' Office of Security and Privacy Oversight to understand its organization and approach to better manage and improve security. Our ongoing efforts have already mitigated over 85 percent of the weaknesses identified in the GAO's 1997 report on security weaknesses. The GAO noted earlier this year that this measurable improvement exceeded its expectation. Normally, the GAO would have considered mitigating 25 percent of the weaknesses a good solid effort.

Working on these weaknesses, while evaluating and identifying new weaknesses and corrective actions at all computing centers, service centers, and district offices has required a substantial resource commitment by the IRS. For example, the Office of Security and Privacy Oversight's operating costs are estimated at about $28 million for this year. This does not include the costs of implementing actions to correct weaknesses, such as implementing physical security upgrades that were funded at approximately $21 million, $15 million, and $9 million in 1997, 1998, and 1999, respectively. For 2000, we estimate that $9 million will be used for physical security improvements.

As is the case with TIGTA and GAO reports, which have also delineated specific weaknesses and vulnerabilities with specific facilities and/or facility types, we are asking that your report be labeled and protected as "Limited Official Use." This is because its distribution increases the risks associated with disclosing the identified weaknesses and vulnerabilities. We recommend that your staff work directly with the Office of Security and Privacy Oversight's Director of the Office of Security Evaluations & Oversight, who can be contacted at 202-283-4500, to discuss the limited distribution of the report and to agree on a redacted version of the report that can be released to the public. In this regard, future draft reports addressing physical and other security weaknesses should be labeled and protected as "Limited Official Use" until the Director of the Office of Security Evaluations & Oversight has assessed it for potential risks associated with the disclosure of the weaknesses and vulnerabilities.

As requested, this letter is not a "Limited Official Use" document. Neither is its attachment, which addresses the two high-level recommendations in TIGTA's draft report. As discussed above, however, we have designated your draft report as a "Limited Official Use" document. In this regard, it should be restricted to only officials with a "need to know" and should not be released publicly.

In closing, thank you for assisting our efforts to improve the IRS' physical security capabilities. We ask that you include a copy of this response and its enclosure in your "Limited Official Use" and redacted versions of your final report. If you have any questions, or if you would like to discuss this response in more detail, please contact, Len Baptiste, Director of the Office of Security and Privacy Oversight at 202-622-8910.

Attachment

Responses to TIGTA's November 4, 1999 Draft Audit Report, entitled The Internal Revenue Service Can Improve Information Systems Physical Security

Following are the responses to the two recommendations in TIGTA's Draft Audit Report, entitled The Internal Revenue Service Can Improve Information Systems Physical Security, dated November 26, 1999.

Recommendation # 1

The Chief Information Officer, in conjunction with other IRS executives and field managers, should ensure that minimum physical security requirements for information systems operations are met in the IRS' facilities.

The executives need to take steps to address the specific weaknesses identified in this report. They also should perform reviews in all IRS locations to assess the state of physical security and take steps to reduce similar exposures in those locations. This will require IRS management to prioritize the need to reduce these exposures, including seeking and obtaining funds to correct the weaknesses.

- In performing these reviews and prioritizing the corrective actions necessary to address security weaknesses, IRS management needs to consider the risks and assume responsibility if they do not take corrective actions. To implement these activities, we suggest that:

- The IS, Support Service and Compliance functions use existing guidelines and controls to review the state of physical security in their facilities and implement their respective requirements for physical access, fire protection, and environmental controls.

- The IRS' organizational components follow existing procedures for properly storing magnetic media and for conducting tape inventory validations. (The inventory process includes reporting inventory results to the IRS National Office Field Systems and Support Branch. The process includes reconciling and resolving inventory discrepancies and performing vulnerability studies for missing tapes.)

Assessment of Cause

Prior to 1997, the IRS reduced its investments in important systemic and physical security initiatives because of financial and operational considerations. During this period, the IRS support budgets—excluding training—decreased by over 14 percent in 4 years. Faced with difficult investment choices, the Service believed that it made wise management decisions between operational and security priorities. However, the IRS also recognizes that security enhancements were needed to ensure that integrated and consistent safeguards are in place to adequately ensure the (1) privacy and security of taxpayer account information,

Page 1 of 4

(2) continuity of its operations, and (3) security of the infrastructure for modernized systems.

Since 1997, major improvements have been made in improving the IRS' physical security. For example, it implemented physical security upgrades that were funded at approximately $21 million, $15 million, and 9 million in 1997, 1998, and 1999, respectively. For 2000, it is estimated that $9 million will be used for physical security improvements. It should be noted that this is a very large multi-year effort that originally focused on the IRS' more critical facilities, which pose the biggest risks if physical security is breached. Actions are currently underway to also improve other facilities, while still focusing considerable efforts at maintaining adequate security postures at the critical facilities. It also should be noted that many of the corrective actions take years to complete, so risks associated with not having them complete and with not reviewing all facilities will continue to have to be managed through priorities. Again, the IRS' approach is focused on substantially reducing this risk over the next few years.

Corrective Action

The Office of Security & Privacy Oversight's Director of the Office of Security Evaluations and Oversight, in conjunction with other IRS executives and field managers, will continue its aggressive efforts to establish minimum physical security requirements for information systems operations at all IRS facilities.

Whereas no program can provide a risk-free security infrastructure, the IRS is focused on a disciplined management approach of preventing, detecting, and reacting to serious weaknesses. As in any entity, the resources available for security enhancements and upgrades are prioritized to first deal with high-risk and sensitive areas, because not all weaknesses identified by the IRS or others are equally serious. Some may not be serious at all—especially if corrective actions in other areas provide compensating controls, or if the weakness does not necessarily increase any additional risk. For example, the risk associated with TIGTA's finding that locations do not have plastic covers to shield computers when fire sprinklers activate is an antiquated approach, which over time has not proven to be beneficial.

The Office of Security Evaluations and Oversight currently performs about 150 reviews at various facility types each year. It also is acquiring contractor support to help with its effort. However, these security efforts will not focus on visiting the over 1,000 IRS facilities in the short term. Instead, it will continue to work issues following its disciplined facility-type approach, which is asset based, and to initiate facility-wide improvements where such actions are decided to be high enough priorities. Changing this approach, which GAO has agreed is very effective would risk the Service's ability to continue making substantial improvements, which is an established goal of the program. In this regard, the IRS believes that with its current security approach, it is adequately identifying,

managing and mitigating risks. It is also making a large financial commitment to maintain its efforts, while it also continues to work with Treasury and its other bureaus to obtain additional security funds for critical infrastructure protection. To date, however, no additional funding sources have been identified.

Summary of Action for ITC

The Office of Security & Privacy Oversight's Director of the Office of Security Evaluations and Oversight, in conjunction with other IRS executives and field managers, will continue its aggressive efforts to establish minimum physical security requirements for information systems operations at all IRS facilities.

Implementation Date

December 16, 1999

Responsible Officials

Director, Office of Security Evaluations & Oversight

Recommendation # 2

The executives need to use the Office of Systems Standards and Evaluation to evaluate the progress the IRS has made in meeting plans to reduce or eliminate the identified exposures.

Assessment of Cause

Prior to 1997, the IRS did not have a centralized office responsible for oversight of security. It also had not committed needed resources to conduct comprehensive security reviews. The IRS initiated an aggressive security management program in January 1997, when it established its Office of Systems Standards and Evaluation. Now called the Office of Security and Privacy Oversight (SPO), this Office's responsibilities include establishing and enforcing standards and policies for all major IRS security programs including, but not limited to, physical security, data security, systems security, and personnel security.

Corrective Action

The Office of Security Evaluations and Oversight currently performs about 150 evaluations at various facility types each year. As part of these reviews, Security Evaluation and Oversight conducts follow-up reviews to assess progress that sites are making in mitigating identified security risks. In addition to these follow-

up reviews, the office conducts problem-solving visits to work directly with local staff to develop and implement viable corrective actions to mitigate the risks.

Summary of Action for ITC

The Office of Security Evaluations and Oversight currently performs about 150 reviews at various facility types each year. As part of these reviews, Security Evaluation and Oversight conducts follow-up reviews to assess progress that sites are making in mitigating identified security risks. In addition to these follow-up reviews, the office conducts problem-solving visits to work directly with local staff to develop corrective actions for unresolved risks.

Implementation Date

December 16, 1999

Responsible Officials

Director, Office of Security Evaluations & Oversight