Persistent Security Weaknesses at Internet Connections Can Be Traced to a Lack of Policies and Procedures

August 2002

Reference Number: 2002-20-145

TD P 15-71

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 5, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Persistent Security Weaknesses at Internet Connections Can Be Traced to a Lack of Policies and Procedures (Audit # 200220032)

This report presents the results of our review to determine the underlying reasons for security weaknesses at Internet connections. In the past 18 months, we have conducted reviews of four Internet connections and found significant weaknesses at each. We performed this review to comply with the Internal Revenue Service (IRS) Restructuring and Reform Act of 1998,[1] which requires the Treasury Inspector General for Tax Administration (TIGTA) to assess the adequacy of IRS computer security controls.

In summary, we found that the weaknesses we identified in our prior reports could enable hackers to gain access into the IRS' internal networks. Once inside, they could access sensitive files (including taxpayer data) from several systems on the network, plant malicious programs to gain further access or destroy information, or hinder network performance by causing a denial of service.

Collectively, the weaknesses we found illustrate the consequences of poorly managed and uncontrolled Internet connections. Aside from specific causes at each connection, we believe these weaknesses persist because the IRS has too many Internet connections and it has not established policies and procedures to standardize the connections.

---

[1] Pub. L. No. 105-206, 112 Stat. 685 (1998).

We recommend that the IRS reduce the number of Internet connections it maintains, assign accountability for managing all Internet connections to one office, develop and implement penalties for unauthorized or unapproved connections going outside the IRS, and standardize all current and future Internet connections.

Management's Response: Management's response was due on July 18, 2002. As of July 30, 2002, management had not responded to the draft report.

The TIGTA has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Persistent Security Weaknesses at Internet Connections Can Be Traced to a Lack of Policies and Procedures

Background

The Internal Revenue Service (IRS) uses external connections to conduct many tax administrative activities. For example, the IRS has established:

- Internet web sites that allow the public and tax practitioners to access tax-related information.
- Extranet[1] connections that allow certain Government agencies or contractors to share information or services.
- Dedicated connections that allow employees to access third party sources for tax and legal research purposes.

While these connections can facilitate business operations and increase productivity, they also pose significant risks because each connection represents an entry point into the IRS' computer architecture. The IRS must maintain adequate security at each connection to ensure that the traffic passing through each connection is authorized.

Security weaknesses at Internet connections give hackers the opportunity to exploit and gain unauthorized entry into the internal network. If hackers can get into the internal network, they can cause damage in many ways, such as accessing sensitive files (including taxpayer data) from several systems on the network, planting malicious programs to gain further access or destroy information, or hindering network performance by causing a denial of service.

The Department of the Treasury and the National Institute of Standards and Technology (NIST) have issued guidance on security at Internet connections. Generally, well-configured firewall computers and routers provide preventive measures against attacks, while intrusion detection systems provide detection mechanisms for attacks.

[1] Extranet connections are generally Internet web sites that are targeted at a specific group of users and often incorporate the use of a username and password to access the site.

We conducted this review to comply with the IRS Restructuring and Reform Act of 1998[2], which requires the Treasury Inspector General for Tax Administration (TIGTA) to assess the adequacy of IRS computer security controls. We conducted this audit from November 2001 to April 2002 in IRS National Headquarters offices in Washington, D.C., and New Carrollton, Maryland. The report also includes issues identified during prior TIGTA audits of IRS Internet connections from 2001 and 2002.

The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Security Weaknesses Existed at Internet Connections into the Internal Network

We previously reported on several security weaknesses at Internet connections[3] into the IRS' network architecture. These weaknesses left the IRS unnecessarily vulnerable to attacks by hackers. Appendix IV provides a list of the four previous TIGTA reports issued on Internet connections and a compilation of the security weaknesses reported.

- The IRS had not installed firewall computers and intrusion detection capabilities at all connections. Firewall computers that had been installed were not optimally configured and maintained to minimize the possibility of an attack. Also, vulnerabilities, well known by hackers, had not been patched. In addition, administrators allowed unnecessary telecommunications traffic to enter the IRS network and provided opportunities for hackers to change settings remotely.
- Physical security over firewalls, routers and intrusion detection equipment was often weak. Password controls on key equipment were also weak. These deficiencies could allow unauthorized personnel to access connection

[2] Pub. L. No. 105-206, 112 Stat. 685 (1998).

[3] For readability purposes, we use the term "Internet connection" when referring to the connections within the scope of this report. While the IRS maintains both Internet and dedicated connections, a majority of the external connections use the Internet as the means for connectivity.

components and make unauthorized changes to the components.

- Activity logs, records of configuration changes, and audit trail logs were not maintained. Without this information, the IRS was hindered in identifying and investigating potential attacks.

We made recommendations in the prior reports to correct these site-specific weaknesses and the IRS responded with adequate corrective actions. However, these persistent weaknesses indicate underlying causes that need to be addressed.

Internet Connections Have Been Poorly Managed

We believe these security weaknesses persist because the IRS has too many Internet connections and has not established policies and procedures to standardize the connections.

The IRS has too many Internet connections

Ideally, an organization the size of the IRS should have only one or two Internet connections. The IRS knows of at least 24 Internet connections and its business units have proposed 17 new connections. The IRS has not evaluated its Internet connections to determine if they could be consolidated. An official in the Office of Security Services indicated that this is the direction to head, but little progress has been made.

Combining Internet connections would reduce security vulnerabilities, simplify maintenance, and reduce costs associated with Internet connections.

Reduce Security Vulnerabilities The greater the number of Internet connections, the greater the opportunities for hackers to steal taxpayer data since each connection represents another avenue into the IRS' internal network. Based on the control weaknesses we identified above, we believe the number of current connections is an unacceptable risk.

Simplify Maintenance Based on our prior audits, the IRS has had difficulty updating components with the latest security patches. Reducing the number of connections would reduce the number of components to be maintained.

Typically, each Internet connection consists of various components, with a minimum of two routers or switches (internal and external), two firewall computers (internal and external), and an intrusion detection server with two sensors (internal and external). Each component requires maintenance to ensure its continual operability and maximum protection. If each of the 24 known connections had these components, the IRS would need to perform maintenance on at least 168 components, not including specific components required at certain connections (e.g., web servers for web sites and extranet sites). With fewer connections, monitoring to detect intrusions would be improved and unusual or questionable traffic patterns could be easier to identify.

Reduce Costs Costs include staffing needed to maintain and monitor connections and other support costs (e.g., fees to third-party Internet Support Providers and costs for telecommunication lines). Costs to support an Internet connection can range from a few thousand dollars for a more primitive system to hundreds of thousands of dollars for the more advanced systems.

We had some difficulty in obtaining specific reasons for the current number of Internet connections due to a lack of historical information on the connections. Most of the Internet connections were created prior to the IRS' reorganization efforts. At that time, the IRS operated in a decentralized and autonomous manner. Typically, field and functional executives had almost total control over their offices, including the Information Systems organizations. This decentralized approach allowed for connections to be set up based on local approvals without coordination with and knowledge of the Chief Information Officer's staff.

The lack of a formal policy for establishing Internet connections, including procedures for ensuring all external connections are centrally controlled and approved, played prominently in the IRS' current predicament. The lack of these policies and procedures has created a situation where even the Deputy Commissioner for Modernization and

Chief Information Officer's staff is unsure of the number of connections that exist.

When we conducted an opening meeting for our first audit of an Internet connection in November 2000, officials with the Enterprise Network Management Office (formerly the Office of Telecommunications) knew of nine Internet connections. After the Office of Mission Assurance was given responsibility for security of the connections in May 2001, it began efforts to identify all external connections to the IRS' network. As of December 2001, the IRS acknowledged that it has at least 24 Internet connections. Though it believed that it had identified all of these connections, it was not absolutely sure.

During this review, the Office of Mission Assurance was not able to provide us with detailed information on each of the 24 connections. This included which function was responsible for the connection, who was the main functional contact point for the connection, what was the purpose of the connection, and what type of components were used for the connection.

The need for these policies and procedures still exists. An official with the Office of Mission Assurance stated that informal requests via electronic mail are sometimes used to request external connections. Officials with the Enterprise Network Management Office mentioned the Certification and Accreditation process[4] as another way to open connections. The IRS has no single authority or approval point for external connections.

The Deputy Commissioner for Modernization and Chief Information Officer has not been aggressive enough in wresting control of the existing Internet connections from business unit executives. We believe he needs to take a

[4] The Certification process provides a comprehensive evaluation of security features to ensure the system meets a specified set of security requirements. The Accreditation process is the official declaration that the system owners accept the security risks related to the system's operation, based on the results of the certification process. These processes provide proof that adequate security exists on the system to ensure the integrity, confidentialty, and timeliness of sensitive data.

more active role to minimize the significant risks associated with opening so many Internet connections.

The IRS has not established a standard configuration for Internet connections

Because no standard security configuration exists, project offices, or in some cases contractors who install Internet connections, are left to determine the hardware and software security configurations for each connection. Each of the 4 connections we reviewed had different configurations and it is likely that the other 20 connections are also different.

The lack of a standard configuration greatly increases the difficulty in managing Internet connections and significantly increases the risk that they will be hacked. For example, administrators have a difficult enough time keeping up with the security patches for one hardware/software configuration. The difficulty increases with the number of configurations making it more likely that a patch will not be installed and that a hacker will find the vulnerability.

The IRS has no specific guidance to ensure that Internet connections are securely configured. The Office of Mission Assurance cited that the Internal Revenue Manual contains information on Internet security. While there are sections pertaining to Internet connections, the text provides general guidance as opposed to formal policies and procedures for ensuring security at the connections.

Several authoritative organizations[5] have cited the importance of establishing security standards and policies prior to implementing connection security. These standards

[5] The NIST, a federal organization that provides guidance for government agencies on Information Systems areas, published Special Publication 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*. Also, the System Administration, Networking, and Security (SANS) Institute has several guidance documents on security standards at Internet connections. SANS is a cooperative research and education organization, in which over 96,000 industry professionals share the lessons they are learning and find solutions for challenges they face. The core of the Institute consists of security practitioners.

should be used as a guide to ensure adequate protection at connections.

The IRS has taken some steps to address standardization. For example, the Deputy Commissioner for Modernization and Chief Information Officer transferred responsibilities of the firewall and intrusion detection infrastructure from the Enterprise Network Management Office to the Office of Mission Assurance under the Chief, Security Services. The Director, Office of Mission Assurance, has indicated that actions are underway to replace all firewalls with standardized hardware and software as part of the IRS firewall program. In addition, Web Services has been tasked with the development of policies and standards for the web environment. Guidance is expected to be in place by October 2002.

These are positive steps, but we believe the IRS is moving too slowly. The IRS' response to our report on the first external connection we reviewed stated that the Office of Cyber Security (now the Office of Mission Assurance) would develop and implement Internet security policies by October 2001 for that particular connection. At the date of this report, it still did not have a policy statement to share with us.

In May 2001, concerns over the IRS' external connection environment were brought forward at a Technology Security Committee meeting from the Office of Mission Assurance. The minutes for that meeting indicated that the decision was made to come up with a plan to address the issues. Subsequent meetings did not mention any follow up to the original actions that were to be taken.

Recommendations

The Deputy Commissioner for Modernization and Chief Information Officer should:

1. Reduce the number of Internet connections to a more manageable number, and develop and implement a formal migration plan to achieve this goal. To ensure continuity of operations in the event of a failure, we

suggest attempting to limit the total number of Internet connections to two. In the meantime, immediately suspend implementation of all new external connections into IRS networks.

2. Assign accountability for managing all Internet connections to the Office of Mission Assurance and establish procedures for users when requesting Internet connections.

3. Develop and implement penalties for unauthorized or unapproved connections going outside the IRS. Unauthorized connections jeopardize the entire IRS network and the confidentiality and privacy of all taxpayers' records. Penalties should be sufficiently severe to deter any IRS manager or employee from opening an Internet connection without the authorization of the Deputy Commissioner for Modernization and Chief Information Officer.

4. Standardize all current and future connections. Implement firewalls and intrusion detection systems at all existing and future external connections and develop standard security configurations.

Management's Response: Management's response was due on July 18, 2002. As of July 30, 2002, management had not responded to the draft report.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to determine the underlying reasons for significant weaknesses at Internet connections.[1] We accomplished our objective by conducting the following audit tests.

I. We evaluated the processes over how the IRS establishes and monitors external gateways.

- A. We identified Government and Industry guidance and standards for external connections.
- B. We identified IRS policies and procedures over external connections by researching the Internal Revenue Manual and other IRS guidance information and interviewing IRS personnel from Telecommunications and the Office of Security Services.
- C. We determined if IRS policies and procedures over external gateways had been adequately documented and distributed to employees for awareness and adherence.

II. We profiled the existing external gateways maintained by the IRS to determine whether it effectively controlled and managed them.

- A. We identified existing IRS external gateways from prior TIGTA audit workpapers and by consulting with the Offices of Security Services and Telecommunications.
- B. We contacted IRS contractors to obtain background information regarding certain gateways.

III. We compiled issues from four prior TIGTA audits of external gateways.

[1] For readability purposes, we use the term "Internet connection" when referring to the connections within the scope of this report. While the IRS maintains both Internet and dedicated connections, a majority of the external connections use the Internet as the means for connectivity.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Bret Hunter, Senior Auditor
Ted Tomko, Senior Auditor

Appendix III

Report Distribution List

Commissioner N:C
Deputy Commissioner N:DC
Chief, Security Services M:S
Director, Enterprise Network M:I:E
Director, Mission Assurance M:S:A
Deputy Chief Financial Officer, Department of the Treasury

Appendix IV

Previously Issued Reports on Internal Revenue Service Connections and Security Weaknesses Reported

We have issued four reports that address connections into the Internal Revenue Service's (IRS) network architecture.

- *Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2001-20-101, dated June 2001).
- *Controls Over the Procurement Web Site Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2002-20-045, dated January 2002).
- *Controls Over the LexisNexis Connection Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2002-20-063, dated March 2002).
- *Controls Over the Excise Files Information Retrieval System Web Site Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2002-20-064, dated April 2002).

Cited in these reports were several security weaknesses, which have been compiled below.

Firewalls and/or intrusion detection systems were not in place

The IRS had not implemented a firewall computer at one external connection. As such, there was no preventive barrier at this connection against external attacks. In addition, the IRS had not installed intrusion detection systems at three external connections. The IRS cannot identify external attacks without adequate intrusion detection systems.

Vulnerabilities in firewalls and/or routers were not patched[1]

The IRS took no action to assess and correct vulnerabilities in firewall systems at three external connections. Correcting these weaknesses is critical since these types of vulnerabilities are known publicly and discussed on both vendor and hacker web sites. Unpatched vulnerabilities can be exploited by hackers to take control of the firewall or disable it all together.

[1] A patch is a quick-repair job for a piece of programming. The patch is not necessarily the best solution for the problem and the product developers often find a better solution when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in programming code.

Unnecessary services were running on firewalls

Unnecessary services were running on the firewall computers at three external connections. One of the unnecessary services was the ability to access the firewall computers from any computer connected to the Internet by anyone with the administrator account and password, and several contractors and former employees knew this information. Similar to unpatched vulnerabilities, unnecessary services can be exploited to take control of or disable the firewall.

Too many types of traffic were allowed

The firewall computer was configured to allow too many types of traffic at one external connection. For example, the firewall allowed traffic with internal Internet Protocol addresses to come from the outside. This weakness could allow hackers to launch "spoofing" attacks.[2] Allowing too many types of traffic gives hackers more opportunities to gain entry into the IRS' internal network.

Firewall software was outdated

Outdated firewall software was running that was no longer supported by the vendor at one external connection. The lack of vendor support means that new vulnerabilities with this software were not addressed, which could provide hackers with a means to exploit the firewall.

Firewall system maintenance was not performed

General maintenance of system components was not performed on two external connections. For example, sample tutorial files remained on the web servers. Hackers can use this information to perform denial of service attacks. Also, criminal actions against hackers may be jeopardized because the web server and firewall clocks were not synchronized with each other. Maintenance on the firewall maximizes the protection capabilities against hackers.

Firewall system and/or router configuration changes were not documented

Firewall system configuration changes were not documented and maintained at three connections. The IRS had no record of changes and did not know if only authorized changes were made to the firewall computers and routers. Configuration management is fundamental in gaining control over firewall and router activities.

Firewall and/or router activity logs were not completely retained or reviewed

Firewall system activity logs were not completely retained, backed-up, and/or reviewed for potential security breaches at two external connections. We found that some firewall logs were missing for certain periods of time. The IRS had not reviewed the logs that did exist for questionable activities or connections. Maintaining and reviewing activity logs is important in

[2] Spoofing occurs when a hacker masquerades his/her computer as a legitimate computer on the network, thus fooling the router into thinking that the connection is coming from a trusted source.

identifying questionable traffic and in providing footprints while investigating potential hacker activities.

Audit trails were not enabled or reviewed for components

Audit trail controls were either not enabled or reviewed for the components at two external connections. When used appropriately, audit trails provide documentation on all access activities by users and administrators. This information provides chronological history of who did what and when. By not reviewing audit trail data, unauthorized accesses or questionable activities would go undetected.

Password and user account controls on firewalls and routers did not limit access

Password controls and user accounts did not restrict access to only those with a need to know at three external connections. Some routers and firewalls had only one generic user account with a password shared by its administrators. Also, the password for the router was not always encrypted. The generic user accounts limited the accountability over changes made, and unencrypted passwords exposed the IRS to possible system hacking. By not limiting access to the firewall and router, unauthorized changes to firewall and router configurations can be made and expose the connection to hackers.

Physical access was not restricted

Physical access to the computer rooms was not always restricted to only those who had a need for such access at one external connection. Management did not receive monthly activity reports to review and identify individuals who no longer needed access to computer rooms. By not limiting physical access to the firewall and router, unauthorized individuals can attempt to access the components and make changes to configurations.