Sensitive Technology Information Was Posted on the Internet

February 2004

Reference Number: 2004-20-046

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 27, 2004

MEMORANDUM FOR CHIEF, MISSION ASSURANCE
CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Sensitive Technology Information Was Posted on the Internet (Audit # 200320041)

This report presents the results of our review to determine whether sensitive Internal Revenue Service (IRS) information could be obtained on the Internet.

In summary, sensitive information relating to IRS computer systems was posted on the IRS' Internet web sites and third-party web sites. This information included detailed Modernization blueprint documents and the Internal Revenue Manual on Information Technology (IT), which the IRS has designated as Official Use Only (OUO). We also found several newsgroup postings that divulged specific hardware and software used by the IRS, including detailed information regarding a major production system. With this information, a hacker would have a better opportunity to successfully attack the IRS' infrastructure and potentially gain access to taxpayer information.

The IRS can control information on its web sites and, to some extent, what is available on third-party web sites. The information posted to third-party web sites appears to have been gleaned from the IRS' own web sites and from presentations given by IRS employees.

Neither the employees responsible for providing information for Internet sites nor the employees responsible for adding the information to the web sites evaluated the sensitivity of the information, other than to ensure taxpayer information was not posted. The IRS has no guidelines to assist employees in assessing security risks before posting information on the Internet.

The IRS Office of Mission Assurance has initiated efforts to establish standardized procedures and guidelines for reviewing and classifying sensitive information, which includes information to be posted on the Internet. As of December 2003, this Handbook was in draft format. The draft Handbook addresses the issue of unnecessarily posting

sensitive information on the Internet, but does not contain specific examples of what should and should not be allowed.

The risk of divulging sensitive information could also be limited if employees complied with the IRS' Internet usage policy. The Internet policy prohibits the posting of agency information to existing sites without approval from the appropriate management official.

We recommended that the Chief, Mission Assurance, continue efforts on finalizing the procedures, guidelines and training material for identifying sensitive information; coordinate with the Office of Electronic Tax Administration, the Office of Servicewide Policy, Directives, and Electronic Research, and the Office of Governmental Liaison and Disclosure to distribute the guidelines throughout the IRS; and periodically remind all employees and contractors of the IRS' Internet Usage Policy. For the Procurement web site, we recommended that the Chief Information Officer restrict access to sensitive contracting information by assigning user accounts and passwords to only those with a need to know.

Management's Response: The Chief, Mission Assurance, concurred with our recommendations. The Office of Mission Assurance will finalize guidelines for identifying OUO information, develop training modules for use by document owners, ensure training material is fully integrated in existing policies and procedures, and include special emphasis on disclosure of IT information in its annual Security Awareness training. To restrict sensitive technical information on the Procurement web site, the Director, Procurement, has implemented the Federal Technical Data Solution, a web-based application that uses user accounts and passwords for access. Management's complete response to the draft report is included as Appendix IV.

Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Sensitive Technology Information Was Posted on the Internet

Background

The Internet offers a vast library of information to millions of computer users. The Internal Revenue Service (IRS) makes wide use of the Internet to provide important information to the general public and to contractors interested in conducting business with the IRS. To facilitate effective customer service, the IRS has placed many of its policies and procedures on the Internet to assist taxpayers and practitioners.

The Internet has no rules governing the content of information available to users, and virtually anyone can post information to web sites. As a result, the IRS is faced with the risk that employees could knowingly or unknowingly make sensitive information available to the public.

Although there are other avenues used to share information, such as IRS-sponsored tax forums and public briefings, we focused our review on sensitive IRS technology information available on the Internet. Hackers routinely search the Internet for useful information prior to attacking a target organization. For example, if a hacker can identify the type of hardware or software used by an organization, he or she could potentially exploit the known vulnerabilities associated with those components. The IRS must be particularly mindful of the security risks associated with posting technology information on the Internet to prevent unauthorized access to tax information.

This audit was conducted at the IRS National Headquarters in Washington, D.C., from June through December 2003 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.

Sensitive Internal Revenue Service Information Is Available on the Internet

Sensitive information relating to IRS computer systems was posted on the Internet. Applying the same techniques we used, hackers can easily find this information and use it to attack the IRS' infrastructure and potentially gain access to tax information.

We categorized our results into three areas. Specifically, sensitive information was:

- Posted on IRS Internet web sites.

- Communicated by IRS employees on Internet newsgroups.
- Posted by outsiders on the Internet.

The IRS can control information on its web sites and, to some extent, what is available on third-party web sites by establishing policies and guidelines for protecting sensitive IRS information. The risk of divulging sensitive information, however, is directly dependent on employees' familiarity and compliance with those policies and guidelines.

Sensitive information posted on IRS web sites

An agency's most direct path for providing information to the public is often its own Internet web site. Agencies must strike a balance between providing appropriate information and offering too much information. We searched through the IRS' two public web sites[1] and identified information that we believe should not have been available to the public.

Specifically, on the IRS Procurement web site, we identified:

- IRS Modernization blueprint documents. These documents contained information on the IRS' infrastructure, including hardware and software to be used in specific Modernization projects.
- The Internal Revenue Manual (IRM), Part II, Information Technology. In September 2002, the IRS Technology Security Committee decided to reclassify this section of the Manual as Official Use Only (OUO) and remove it from public access. The Manual contains sensitive technology information, including password policy and computer operating systems and software used.

[1] The two IRS web sites accessible for public use are the IRS' Procurement web site and the IRS' Digital Daily. There are other IRS web sites designed for specific business purposes, and they are restricted from general public viewing.

- IRS internal Internet Protocol addresses and Domain Name System names, along with the platforms and applications used.
- IRS floor plans of a computing center. This document contained the location and the number of IRS occupied floors, including the computer room location.

On the IRS Digital Daily web site, we identified:

- The Statistics of Income (SOI) computer infrastructure. An SOI web page presented a recruiting announcement that contained specific information on computer platforms, operating systems, and applications used within its office. The SOI web pages also identified office locations.

Both Procurement and SOI personnel stated they only performed a cursory review of the documents and did not consider the inherent security risks associated with the information we found. Procurement personnel stated that their role is to serve as the administrative function for placing the contents onto the web page. They also stated that business units dictate the contents of their postings, especially for contract solicitations. Business unit owners stated that they did not review for, and were not aware of, the risks of posting sensitive information, though they did ensure they did not disclose taxpayer information.

The Department of Homeland Security requires executive branch agencies to develop procedures to "identify and safeguard homeland security information that is sensitive but unclassified" and recently proposed regulations designed to protect critical infrastructure information from disclosure to the general public. The IRS had no policy or guidelines for information being posted to agency web sites regarding security concerns. The Electronic Tax Administration office developed local procedures on content reviews for the IRS' Digital Daily, but the procedures did not address security risks.

The IRS Office of Mission Assurance has drafted a Sensitivity Handbook to standardize procedures and guidelines for reviewing and classifying sensitive information, including information to be posted on the

Internet. The Handbook, still in draft as of December 2003, addresses the issue of unnecessarily posting sensitive information on the Internet, but does not contain specific examples of what should and should not be posted. The Mission Assurance senior advisor assigned to oversee the development of the Handbook stated that they are aware of this deficiency and are in the process of developing training modules to address the technical and social issues related to posting sensitive information on the Internet.

Sensitive information communicated by IRS employees on newsgroups

IRS employees can also post agency information on Internet newsgroup web sites.[2] Internet newsgroups provide an open forum where any Internet user can post questions or respond to questions posted on the forum. In the IT industry, these newsgroups enable users to share information and get practical solutions to technical computer problems. Generally, users will provide their business email address as their username for these postings.

We found approximately 830 postings where IRS employees posted questions and answers on newsgroup web sites. In all instances, the employees used their official IRS email addresses (employee first name.employee last name@irs.gov).

We judgmentally selected and reviewed 256 of the newsgroup postings and found 84 that contained sensitive IRS computer information. Of the 84 postings, 77 were from @irs.gov authors and 7 were from @ci.irs.gov authors. The postings divulged specific hardware and software used by the IRS, including detailed information regarding a major production system. For example:

- In a Microsoft SQL server newsgroup, an IRS employee stated that she was unable to successfully install service pack 3 to a Microsoft SQL server, version 7.0. A hacker could track this information along with related

[2] Examples of newsgroup web sites include Microsoft (e.g., Microsoft.public.xxx with xxx being a specific MS program) and IBM (e.g., bit.listserv.ibm-main) newsgroups.

information from the National Institute of Standards and Technology web site, which shows there are 11 vulnerabilities with SQL 7.0 running service pack 2.

- In a Microsoft Internet Explorer newsgroup, an IRS employee stated he had attempted to install service pack 1 on Internet Explorer, version 5.5, but ran into problems that he did not encounter without the service pack. A hacker could ascertain from this posting that the IRS had workstations without service pack 1 installed. As of the date of the posting in March 2001, there were 10 published vulnerabilities. As of October 2003, there were 86 published vulnerabilities for this situation.

The risk of divulging sensitive information could be limited if employees complied with the IRS' Internet usage policy. The policy contains strict prohibitions against posting agency information to external newsgroups, bulletin boards, or other public forums without approval from the appropriate management official. The IRS employees were either not aware of the prohibitions or ignored them for the convenience of asking knowledgeable persons outside the IRS for advice. In either case, the security risks were not addressed.

Newsgroup and bulletin board postings are controlled by independent organizations and may be retained on the Internet for a long time. Some of the sensitive information identified during our research dated back to April 1998.

Sensitive information posted by outsiders on the Internet

As part of our review, we conducted Internet searches on certain key words[3] in conjunction with the phrase "IRS." We identified over 68,000 matches when searching for these key words. While judgmentally reviewing over 1,000 of these matches, we identified IRS sensitive information that had been posted on commercial or private web sites. Using this information, a hacker would have a better opportunity

[3] Examples of key words included "firewall," "LEM" (Law Enforcement Manual), "STIR" (Security and Technology Infrastructure Release), and "Oracle."

to attack the IRS' infrastructure. We found the following examples of IRS sensitive information placed by outside individuals or organizations:

- News articles with IRS technology describing the Secure Dial-In project in extensive detail.
- Solicitation for contract work containing sensitive information relating to the IRS' password policy.
- Network diagram of the IRS' Security and Technology Infrastructure Release (STIR) on a non-IRS website illustrated the IRS' three-portal strategy. The STIR is the security architecture for the IRS' modernized systems.
- A section of the Law Enforcement Manual on a non-IRS website.
- A job resumé of a former IRS employee that divulged hardware, software, and versions of IRS computer systems.

These postings were outside the control of the IRS. However, in most of these instances, the information posted appears to have been obtained from the IRS web sites at one time or from other internal sources, such as presentations given by IRS employees. Sufficient attention had not been paid to the security risks of providing sensitive computer information.

Recommendations

The Chief, Mission Assurance, should:

1. Continue efforts to finalize procedures and guidelines for identifying sensitive information. The draft Sensitivity Handbook should address both information provided on the IRS Internet sites and the distribution of information to third parties. We suggest that the Handbook provide examples to demonstrate what information should and should not be posted. Training modules on this material should be developed for use by each business unit.

Management's Response: The Chief, Mission Assurance, will finalize guidelines for identifying OUO information and develop training modules for use by document owners in each business area.

2. Coordinate with the Office of Electronic Tax Administration; the Office of Servicewide Policy, Directives, and Electronic Research; and the Office of Governmental Liaison and Disclosure to ensure that the guidelines are distributed throughout the IRS to Internet content providers, IRM authors, and Disclosure Officers, so they are aware of their responsibilities to identify and properly classify sensitive information prior to posting to the Internet.

   Management's Response: The Chief, Mission Assurance, will coordinate with the offices in our recommendation to ensure that the OUO guidance and training material are fully integrated in existing information classification, document management, and disclosure policies and procedures.

3. Periodically remind all employees and contractors of the IRS' Internet Usage Policy implemented in May 2002. Emphasize the reasons why it is important not to disclose sensitive information, particularly when using newsgroups.

   Management's Response: The Office of Mission Assurance will include special emphasis on disclosure risks related to IT information in its annual Security Awareness training. It will work with the Office of Communication and the Office of Governmental Liaison and Disclosure to develop employee communications in this area in the interim.

The Chief Information Officer should:

4. Restrict access to sensitive contracting information on the Procurement web site to only those with a need to know. We recognize that certain sensitive information is pertinent for the solicitation of contractors and needs to be accessible on the web site. Portions of the web site containing sensitive information should be separated from the general information web pages. In addition, user accounts and passwords should be required to access sensitive areas.

   Management's Response: On October 1, 2003, the Director, Procurement, implemented the Federal Technical Data Solution to post sensitive technical information during the solicitation phase of the acquisition cycle on its web site. This web-based application uses user accounts and passwords to control and restrict access to sensitive information.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether sensitive Internal Revenue Service (IRS) information could be obtained from the Internet.

I. To evaluate the adequacy of security policies and procedures that have been established to guide IRS employees in placing information on the Internet, we:

   A. Reviewed written guidance issued by the IRS and the Department of the Treasury, including Internal Revenue Manual 25.10 (Information Technology Security Policy and Standards), Policy on Limited Personal Use of Technology, IRS Policy on Electronic Communications, Guidance for All IRS Personnel on Internet Access from Government Computers, Treasury Directive 87-04 (Personal Use of Government Office Equipment Including Information Technology), and Guidelines to Identify Sensitive Information.

   B. Researched other related Federal Government guidance, including issuances by the National Institute for Standards and Technology and the General Accounting Office.

II. To evaluate the effectiveness of security policies and procedures implemented for placing information on the Internet, we:

   A. Conducted an Internet search using Google for known hardware and software used by the IRS; for newsgroup postings with authors such as @irs.gov, @ci.irs.gov, @csirc.irs.gov, @irs.treas.gov, and @irs.ustreas.gov; and for other public forums that the IRS employees may post sensitive IRS information technology (IT) security information without authorization.

   B. Identified over 68,000 matches from our Internet search queries. Based on the preview text of the queries,[1] we judgmentally selected and reviewed 256 newsgroup matches and 1,012 other postings for sensitive IRS computer information.

   C. Scanned the IRS' two public web sites – the IRS' Procurement and Digital Daily web sites – for sensitive IT security information.

[1] The Internet search provided results in order starting from the highest to lowest potential for matching the query criteria. We were then able to judgmentally select those matches that contained sensitive information.

D. Contracted with an outside vendor to identify sensitive IRS IT information on the Internet.

E. Contacted IRS personnel to identify security policies and procedures implemented for placing information on the Internet and the reasons why sensitive IT security information was posted on the Internet.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Charles Ekholm, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief, Agency-Wide Shared Services OS:A
Chief, Communications and Liaison CL
Chief, Information Technology Services OS:CIO:I
Director, Electronic Tax Administration OS:CIO:I:ET
Director, Office of Governmental Liaison and Disclosure CL:GLD
Director, Office of Research, Analysis, and Statistics RAS
Director, Office of Servicewide Policy, Directives, and Electronic Research RAS:SPDER
Director, Procurement OS:A:P
Director, Web Services OS:CIO:I:W
Acting Director, Portfolio Management OS:CIO:R:PM
Acting Director, Regulatory Compliance OS:MA:RC
Acting Director, Strategy, Program Management, and Personnel Security OS:MA:SP
Deputy Chief Financial Officer, Department of the Treasury
Audit Liaisons:
    Chief, Mission Assurance OS:MA
    Chief Information Officer OS:CIO:M

Appendix IV

Management's Response to the Draft Report

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

RECEIVED
FEB 13 2004

FEB 13 2004

MEMORANDUM FOR ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Daniel Galik
Chief Mission Assurance OS:MA

SUBJECT: Draft Audit Report – Sensitive Information Technology Data Was Posted on the Internet (Audit # 200320041)

While requiring the development of information classification and management procedures for Sensitive but Unclassified (SBU) homeland security and critical infrastructure information, neither the Office of Management and Budget nor the Department of Homeland Security has developed detailed guidance for executive branch agencies for this effort. Despite the absence of such direction, the Internal Revenue Service has developed significant policy for classification of information, document management, and subsequent information release. IRM 1.9.3, Safeguarding National Security Information and IRM 11.3.12, Classification of Documents are our primary reference sources. As a general rule classification of such SBU information within IRS, Official Use Only (OUO) and Limited Official Use (LOU) category designation, is done by the business owner in conjunction with the Office of Disclosure. Once information receives a classification designation, current policy requires consistent treatment regardless of medium of transmission.

Balancing information sharing requirements, public rights to access, and security/privacy concerns has always been challenging. Nowhere has this been truer than in the area of information technology (IT) data. Your report understandably focuses on this particular category of information, and we concur that there is a need for further guidance in this area. We suggest that you eliminate global references to sensitive IRS information that detract from the IT emphasis in your report.

Unlike Section 6103 data, there are no clear formulas for designating OUO or LOU information technology information. General references to hardware platform types and operating environments do not, in and of themselves, create a sufficient risk to warrant these designations. Even discussions of service pack and patch versions are not necessarily risky in the absence of detailed information on security configurations and system deployments. Of the examples you cited, we agree with your assessment of sensitivity for the IT information on the Procurement web site and on third party web sites only.

I am pleased to inform you that Recommendation 4 of your report has already been fully implemented. With the implementation of the Federal Technical Data Solution (FedTeDS) October 1, 2003, sensitive contracting information is no longer posted on the Procurement web site. FedTeDS is a web-based application that safeguards sensitive technical information during the solicitation phase of the acquisition cycle. It provides user accounts and passwords for access to this information. The Office of Procurement owns and manages the Procurement Web Site and is the responsible business area for this recommendation. Mission Assurance is committed to completing our work, on your other three recommendations, this fiscal year. Please see the attached Corrective Action Plan for more detail.

We appreciate the opportunity to comment on this draft audit report. Please contact me on (202) 622-8910 if you would like to discuss this further. Technical questions may be directed to Deborah England. She can be reached on (202) 622-4561.

Attachment

cc: Director, Procurement OS:A:P
Chief Information Officer OS:CIO
Director, Office of Governmental Liaison and Disclosure CL:GLD
Director, Office of Servicewide Policy, Directives,
and Electronic Research RAS:SPDER
Director, Electronic Tax Administration OS:CIO:I:ET

Management Response to Draft Audit Report – Sensitive Information Technology Data Was Posted on the Internet (Audit # 200320041)

RECOMMENDATION # 1: The Chief, Mission Assurance should - Continue efforts to finalize procedures and guidelines for identifying sensitive information. The draft Sensitivity Handbook should address both information provided on the IRS Internet sites and the distribution of information to third parties. We suggest that the Handbook provide examples to demonstrate what data should and should not be posted. Training modules on this material should be developed for use by each business unit.

CORRECTIVE ACTION TO RECOMMENDATION #1: The Chief, Mission Assurance will finalize guidelines for identifying OUO information. Training modules on the material will be developed for use by document owners in each business area.

IMPLEMENTATION DATE:
October 2005

RESPONSIBLE OFFICIAL:
Director, Assurance Programs OS:MA:AP

CORRECTIVE ACTION MONITORING PLAN:
Overall programmatic responsibility for monitoring implementation of all corrective actions is centralized with the Office of Mission Assurance. Mission Assurance will report program status as part of its Business Performance Review on a quarterly basis.

Management Response to Draft Audit Report – Sensitive Information Technology Data Was Posted on the Internet (Audit # 200320041)

RECOMMENDATION # 2: The Chief, Mission Assurance should - Coordinate with the Office of Electronic Tax Administration; the Office of Servicewide Policy, Directives, and Electronic Research; and the Office of Governmental Liaison and Disclosure to ensure that the guidelines are distributed throughout the IRS to Internet content providers, IRM authors, and Disclosure Officers, so they are aware of their responsibilities to identify and properly classify sensitive information prior to posting to the Internet.

CORRECTIVE ACTION TO RECOMMENDATION #2: The Chief, Mission Assurance will coordinate with the Office of Electronic Tax Administration; the Office of Servicewide Policy, Directives, and Electronic Research, and the Office of Governmental Liaison and Disclosure to ensure that the OUO guidance training material is fully integrated in existing information classification, document management, and disclosure policies and procedures.

IMPLEMENTATION DATE:
Interim OUO Guidance Training Material - October 2004
Final OUO Guidance Training Material - October 2005

RESPONSIBLE OFFICIAL:
Director, Assurance Programs OS:MA:AP

CORRECTIVE ACTION MONITORING PLAN:
Overall programmatic responsibility for monitoring implementation of all corrective actions is centralized with the Office of Mission Assurance. Mission Assurance will report program status as part of its Business Performance Review on a quarterly basis.

Management Response to Draft Audit Report – Sensitive Information Technology Data Was Posted on the Internet (Audit # 200320041)

RECOMMENDATION # 3: The Chief, Mission Assurance should - Periodically remind all employees and contractors of the IRS' Internet Usage Policy implemented in May 2002. Emphasize the reasons why it is important not to disclose sensitive information, particularly when using newsgroups.

CORRECTIVE ACTION TO RECOMMENDATION #3: The Office of Mission Assurance will include special emphasis on disclosure risks related to IT information in its annual Security Awareness training. Further, it will work with the Office of Communication and Government Liaison and Disclosure to develop employee communications in this area in the interim.

IMPLEMENTATION DATE:
September 2004

RESPONSIBLE OFFICIAL:
Director, Assurance Programs OS:MA:AP

CORRECTIVE ACTION MONITORING PLAN:
Overall programmatic responsibility for monitoring implementation of all corrective actions is centralized with the Office of Mission Assurance. Mission Assurance will report program status as part of its Business Performance Review on a quarterly basis.

Management Response to Draft Audit Report – Sensitive Information Technology Data Was Posted on the Internet (Audit # 200320041)

RECOMMENDATION # 4: The Chief Information Officer should - Restrict access to sensitive contracting information on the Procurement web site to only those with a need to know. We recognize that certain sensitive data is pertinent for the solicitation of contractors and needs to be accessible on the web site. Portions of the web site containing sensitive information should be separated from the general information web pages. In addition, user accounts and passwords should be required to access sensitive areas.

CORRECTIVE ACTION TO RECOMMENDATION #4: On October 1, 2003, the Director, Procurement implemented the Federal Technical Data Solution (FedTeDS) to post sensitive technical information during the solicitation phase of the acquisition cycle. This web-based application utilizes user accounts and passwords for access to this information.

IMPLEMENTATION DATE:
Completed - October 1, 2003

RESPONSIBLE OFFICIAL:
Director, Procurement OS:A:P

CORRECTIVE ACTION MONITORING PLAN: Completed.