

**Employees' Extensive Personal Use of the
Internet Should Be Controlled**

November 2000

Reference Number: 2001-20-016

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 17, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Employees' Extensive Personal Use of the
Internet Should Be Controlled

This report presents the results of our review of the use of the Internet in the Internal Revenue Service (IRS). In summary, the use of the Internet offers tremendous research capabilities to IRS employees to assist them in the performance of their jobs. Along with its business application, the Internet offers employees the opportunity to browse web sites for personal reasons. Based on the sample we reviewed, accesses to non-business web sites represented over one-half of all the time employees spent on the Internet. As a result, the IRS is losing productivity, creating unnecessary demand on its telecommunications capacity, and could be fostering a hostile work environment by allowing sexually explicit material into the workplace via the Internet.

We recommended that management enforce the IRS Policy on Electronic Communications by blocking inappropriate sites and monitoring Internet accesses.

Management generally agreed with the findings and their response is included as an appendix. Management's response was incomplete because it did not identify the specific corrective actions to be taken, the responsible officials, and the implementation dates. We will follow up to obtain this additional required information.

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

**Employees' Extensive Personal Use of the Internet
Should Be Controlled**

Table of Contents

Executive Summary.....	Page i
Objective and Scope.....	Page 1
Background	Page 2
Results	Page 3
Employees Were Using the Internet to Access Non-Business Web Sites	Page 4
Conclusion.....	Page 13
Appendix I – Detailed Objective, Scope, and Methodology	Page 14
Appendix II – Major Contributors to This Report.....	Page 17
Appendix III – Report Distribution List.....	Page 18
Appendix IV – Management's Response to the Draft Report.....	Page 19

Employees' Extensive Personal Use of the Internet Should Be Controlled

Executive Summary

Use of the Internet offers tremendous research capabilities to Internal Revenue Service (IRS) employees to assist them in the performance of their duties. We estimate that almost 16,000 IRS employees use the Internet, with potential expansion to the rest of the 97,800 IRS employee population. Providing Internet access also carries some risks, one of which is the opportunity for employees to browse web sites for personal reasons. While personal use of the Internet may improve morale and increase employees' research skills, it comes at a cost of lost productivity and increased demand on telecommunications lines. The Department of the Treasury's guidance on Internet use requires employees to use the Internet for official duties only.

We conducted this review to determine whether the IRS complied with the Department of the Treasury policy on the use of the Internet. Near the end of our review, the IRS issued an electronic communication policy that supplemented the Treasury's guidance.

Results

While the Internet has proven to be a useful research tool, more than half of the Internet activity in our sample was for non-business purposes. IRS management made minimal efforts to enforce the guidance provided by the Department of the Treasury. As a result, the IRS is losing productivity, creating unnecessary demand on its telecommunications capacity, and could be fostering a hostile work environment by allowing sexually explicit material into the workplace via the Internet. We referred the most egregious instances of misuse to the Treasury Inspector General for Tax Administration Office of Investigations (OI). The OI is evaluating these referrals for potential legal violations.

Employees Were Using the Internet to Access Non-Business Web Sites

Considering the wide-ranging duties performed by IRS employees, it is conceivable that any web site could be accessed for business purposes. Based on our analysis, however, we estimate that, of the 16,275 hours of transmission time used to request and receive web site data during our 7-day review period, 8,250 hours (51 percent) were for non-business reasons.

We could not project the impact of non-business Internet use on productivity because it was not feasible to review a statistically valid sample of Internet activity. Nor could we measure the impact on telecommunications costs because the IRS did not maintain detailed cost statistics on the different uses of its telecommunications lines, which annually cost approximately \$390 million. However, because there is a fixed amount of

Employees' Extensive Personal Use of the Internet Should Be Controlled

telecommunications capacity, non-business Internet accesses reduce the amount of telecommunications available for official business.

The IRS did not do enough to raise employees' awareness on the costs of misusing the Internet. In addition, management did not effectively use available software to block accesses to inappropriate sites and monitor the use of the Internet.

Summary of Recommendations

The Commissioner should implement procedures and controls to effectively enforce the recently issued IRS policy on electronic communications. The Chief Information Officer should ensure the timely renewal of the software license to block the use of inappropriate sites, starting in the year 2001, and implement controls to monitor the use of the Internet.

Management's Response: Management generally agreed with the findings and their response is included as Appendix IV. Management agreed to focus on using commercially available blocking software, educating employees and managers on employee productivity issues, and performing random checks on usage. However, management's response was incomplete because it did not identify the specific corrective actions to be taken, the responsible officials, and the implementation dates. We will follow up to obtain this additional required information.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Objective and Scope

The objective of our review was to determine whether the IRS complied with the Department of the Treasury policy on the use of the Internet.

The objective of our review was to determine whether the Internal Revenue Service (IRS) complied with the Department of the Treasury policy on the use of the Internet. We selected 7 days from January and February 2000 to analyze Internet activity for the purpose of building a profile on what IRS employees were accessing on the Internet. We focused our analyses on the top 200 web sites accessed by IRS employees for each of the 7 days in our sample. This approach yielded almost 75 percent of all accesses during the 7 days. We also tracked the total transmission time it took to access each web object.

We could not definitively determine whether each Internet access was for business or non-business purposes. This would have required identifying the individual employee making each access and comparing the access to the employee's official job duties. The intent of this review was to provide an overall profile of Internet use, not to identify individual usage. As such, we made assumptions that Internet accesses to certain categories of web sites were for either business or non-business reasons.

We considered the following web site categories business-related: IRS case-related (e.g., locator services, tax and legal research, and IRS industry partners), U.S. government, information technology, travel (e.g., lodging, transportation, and weather), and employee personnel support (e.g., Employee Express and National Finance Center).

Conversely, the following categories of web sites were considered non-business: financial (e.g., banking or stock trading), Internet Service Provider (ISP) chat room and electronic mail (email), shopping (e.g., auctions), sports, sexually explicit, and gambling.

Employees' Extensive Personal Use of the Internet Should Be Controlled

We further refined our criteria for the news outlets, search requests, and streaming media categories¹ to make a business/non-business determination. As an example, for news outlets, we considered accesses to general news (i.e., local, state, national, and international) and business news were for business reasons. We considered accesses to sports, entertainment, and lifestyle news were for non-business reasons.

We conducted our review from January to June 2000 and coordinated the review with the IRS Information Systems Telecommunications headquarters office in Washington, D.C. This audit was performed in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

The Internet provides computer access to an ever-expanding storehouse of electronic information through the mass connection of almost 1 billion networked computers. Internet users can gain access to information without being concerned about where the information is actually stored. Use of the Internet offers tremendous capabilities to IRS employees in terms of access to a wide variety of information sources relevant to their official duties.

Along with tremendous advantages, the Internet provides access to a wide variety of information that may not be consistent with business needs and may be harmful or inappropriate for the workplace. The Department of the Treasury recognized this risk and issued a memorandum on Internet use to all Treasury offices and bureaus in March 1998. Attached to the memorandum was an Internet Use policy that was

The Department of the Treasury policy on Internet use and the IRS Policy on Electronic Communications state that use of the Internet contributes to the accomplishment of official duties.

¹ Streaming media are real-time video or audio Internet sessions.

Employees' Extensive Personal Use of the Internet Should Be Controlled

intended as a first step to disseminate guidance on the subject. The policy made it clear that “use of the Internet contributes to the accomplishment of official duties” and Internet services “may be monitored to detect possible misuse.” The policy continued to state “the use of Treasury-provided Internet access for unofficial and unauthorized use is inappropriate and may be punishable by disciplinary action.”

In June 2000, the IRS issued to all employees its Policy on Electronic Communications, which covered Internet use. This Policy supplemented the Department of the Treasury policy and contained many of the same requirements and responsibilities.

Results

Use of the Internet offers tremendous research capabilities to IRS employees to assist in the performance of their jobs. While the Internet has proven to be a useful research tool, more than half of the Internet activity in our sample was for non-business purposes. IRS management made minimal efforts to enforce the guidance provided by the Department of the Treasury. As a result, the IRS is losing productivity and creating unnecessary demands on its telecommunications lines and could be fostering a hostile work environment by allowing sexually explicit material into the workplace via the Internet.

We referred the most egregious instances of misuse to the Treasury Inspector General for Tax Administration Office of Investigations (OI). The OI is evaluating these referrals for potential legal violations.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Employees Were Using the Internet to Access Non-Business Web Sites

Fifty-one percent of the Internet activities we reviewed involved accesses to non-business web sites.

In our 7-day sample, accesses to non-business web sites represented 51 percent of all Internet activity. Considering the wide-ranging duties performed by IRS employees, it is conceivable that any web site could be accessed for business purposes. However, based on the percentage of accesses we considered non-business, we concluded that the IRS did not comply with guidance on the use of the Internet and that management actions are necessary.

Our 7-day sample showed that almost 16,000 computer workstations² had accessed over 16.7 million web site objects,³ taking over 21,800 hours in transmission time. It is reasonable to assume that one computer workstation represents one employee. We did not convert the number of web site objects into Internet accesses because a single Internet access can consist of several web objects. While most web objects can be linked to their respective access, some cannot, such as web objects representing links to other web sites.

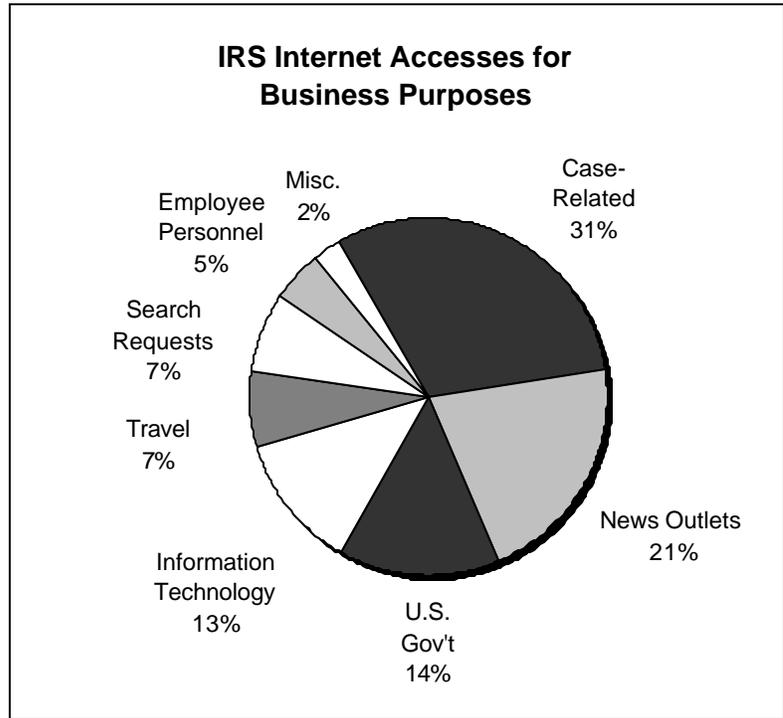
Of the 16,275 hours used for accesses to the top 200 Internet web sites accessed in our 7-day sample, 8,025 hours (49 percent) were for accesses to business-related web sites and 8,250 hours (51 percent) were for accesses to non-business web sites.

² We had to estimate the total number of computer workstations because some workstations that initiated accesses to the Internet were grouped under one identification number and could not be identified separately.

³ When Internet users access a web site, they are actually downloading images from the web site server. These images, which can be in the form of a picture, text document, or advertising banner, were captured as web site objects in our population.

Employees' Extensive Personal Use of the Internet Should Be Controlled

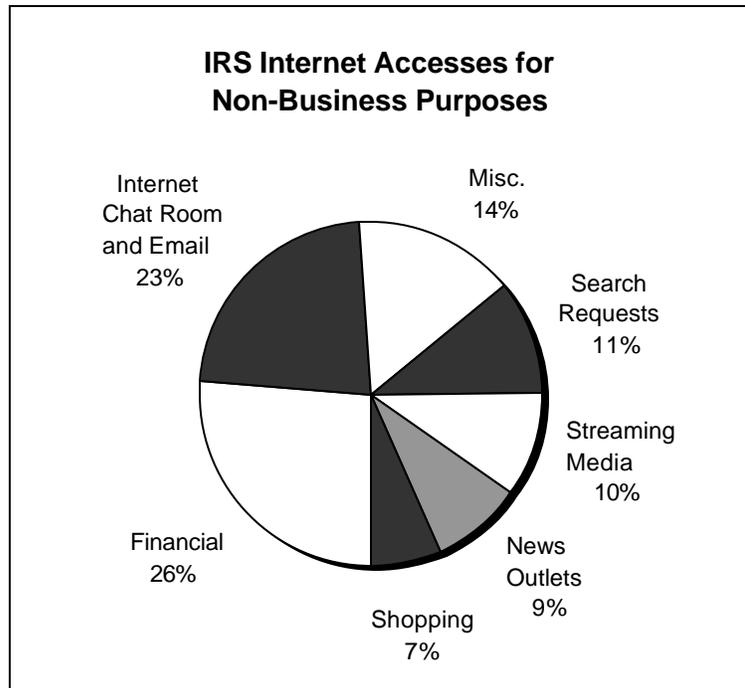
The following chart presents the percentage breakdown of the types of business-related web sites accessed by IRS employees. The percentages were based on the time expended to access these web sites.



As an example of business-related use of the Internet, employees had accessed an on-line public record search web site which provided access to 6 billion public records nationwide. This type of information can be used to locate individuals or businesses and to identify or verify assets of individuals or businesses.

Employees' Extensive Personal Use of the Internet Should Be Controlled

The following chart presents the percentage breakdown of the types of non-business web sites accessed by IRS employees. Like the previous chart, the percentages were based on the time expended to access these web sites.



The Internet Chat Room and Email category represents Internet accesses that allowed employees to communicate with others outside the IRS via an ISP chat room and email transmissions. Because the IRS maintains an official email system for employees, we considered the use of chat rooms and emails through ISP web sites as non-business.

The Non-Business Miscellaneous category consists of accesses to all other web sites that appeared to be for non-business purposes, including sports, sexually explicit, and gambling sites.

Employees' Extensive Personal Use of the Internet Should Be Controlled

We identified 1 IRS workstation where sexually explicit web sites were accessed, on average, 5.5 hours a day during a 21-day period, including 1 day where 14 hours were spent accessing these web sites.

We identified 1 workstation that accessed or attempted to access over 172,000 Internet web objects with over 120 hours of Internet access transmission time during a 21-day period in our January and February 2000 review time frame. Further analysis showed that virtually all of this activity represented accesses to sexually explicit web sites. This usage averaged 5.5 hours per day, including 1 day where 14 hours were spent accessing these web sites.

While Internet accesses to sexually explicit web sites were relatively low (0.4 percent) in our 7-day sample, they are significant because the web site contents may be offensive and could foster a hostile work environment. There were two complaints filed with the Office of Labor Relations in 1999 where male IRS employees had accessed sexually explicit material via the Internet and the contents were inadvertently viewed by female employees.

Non-business use of the Internet can adversely affect employee productivity and telecommunications capacity.

Accessing non-business Internet web sites adversely affects employee productivity and telecommunications capacity. We could not project the impact on productivity because it was not feasible for us to review a statistically valid sample of Internet activity. Nor could we measure the telecommunications costs of using the Internet for non-business purposes because the IRS Telecommunications Division did not maintain detailed cost statistics attributed to various uses of IRS lines. The total annual cost of IRS telecommunications lines is approximately \$390 million.

The effect from personal use of the Internet can also be shown in terms of the bandwidth⁴ needed to allow these types of accesses. Because there is a fixed amount of total bandwidth to support all telecommunications traffic, using the Internet for non-business use can adversely affect performance of business-related activity.

⁴ Bandwidth is the amount of data that can be transmitted through telecommunications lines.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Non-business use of the Internet included video and audio transmissions. These types of Internet sessions can take up to 24 percent of a telecommunications line.

IRS management made minimal effort to restrict and monitor Internet activity of their employees.

One emerging trend for using the Internet is the web site category on streaming media. We determined that 99 percent of the accesses in this category were for non-business purposes. We found non-business video web sessions of a lingerie show, an auto show, and several audio web sessions from music radio stations.

Access to streaming media web sites requires the continual transmission of data between the computer workstation and the web site. The IRS has expressed interest in this technology to deliver training to its employees and to conduct meetings. Our analysis showed that 1 streaming media video session used up to 24 percent of a T-1 telecommunications line⁵ and 1 streaming media audio session used up to 7 percent. Because these types of lines are used to provide geographical connection within the IRS, multiple streaming media accesses can degrade all other telecommunications flow throughout the IRS.

IRS employees were allowed to access the Internet for non-business purposes because IRS management made minimal efforts to restrict and monitor Internet activity. In addition, the IRS had not done enough to raise employees' awareness of the impact of misusing the Internet.

Behind the lack of action by the IRS was the absence of an agency-specific policy on Internet use until June 2000, although there appeared to be much activity around issuing such a policy sooner. The IRS did post the Department of the Treasury policy on the IRS Intranet web site but had done little else to advertise the policy.

In October 1997 (prior to publication of the Internet Use policy issued by the Department of the Treasury), IRS officials had proposed a policy on electronic communications, which addressed Internet use for the IRS. This was in response to an unfair labor practice charge, which was filed on behalf of an employee who had been disciplined for inappropriate use of the

⁵ A T-1 Line is a high-volume telecommunications line.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Internet. An administrative law judge under the Federal Labor Relations Authority ruled against the IRS, partly because it had no policy that clearly stated an employee's responsibility for when using the Internet.

The IRS and National Treasury Employees Union (NTEU) agreed upon terms for the policy on electronic communications in November 1998. The policy was not issued primarily because of a seemingly unrelated disagreement among the Department of the Treasury, IRS, and NTEU over who would pay for computers for the NTEU. An agreement was reached in June 1999, but the Internet use policy was still not issued for 1 year.

IRS officials felt that, without an agency-specific Internet use policy, any monitoring results could not be used to support disciplinary actions and, thus, they did not implement monitoring activities.

Officials with the IRS Information Systems Telecommunications and Security Oversight offices and the IRS Labor Relations office believed that, without an agency-specific Internet use policy in place, monitoring bargaining-unit employees' use of the Internet would be ineffective. Any inappropriate use of the Internet identified through monitoring activities could not be used to support disciplinary actions, as proved by the unfair labor practice lawsuit mentioned above.

Even without an IRS policy on Internet use at that time, the IRS installed Internet blocking software designed to deny access to a pre-determined set of web sites considered inappropriate by the vendor of the software. This control was minimally effective at blocking inappropriate web sites. Based on our analysis, the Internet blocking software restricted access to only 27 percent of the inappropriate web sites that we considered as non-business.

Blocking software designed to block inappropriate Internet accesses was minimally effective.

Because a portion of the blocking criteria is based on pre-determined identification numbers⁶ associated with inappropriate web sites, it is critical that the blocking criteria list contains current information. Similar to how telephone numbers are distributed, when a web site is taken off the Internet, its identification number can be

⁶ All web sites have pre-determined identification numbers (i.e., Internet Protocol addresses) that identify the web site and its location within the World Wide Web.

Employees' Extensive Personal Use of the Internet Should Be Controlled

reissued to another new web site. With an estimated 160,000 new web sites being registered each month, web site identification numbers change at an extraordinary pace.

The licensing agreement purchased with the blocking software allowed the IRS to continually receive updates to the blocking criteria list for inappropriate web sites. However, the IRS' licensing agreement with the vendor expired in December 1999, and the IRS did not timely procure its extension of the license. The licensing agreement was renewed in June 2000. Without the updates, the effectiveness of this control was greatly reduced.

The IRS maintained or had the ability to maintain information to actively monitor Internet activity by its employees but did not do so.

In addition to the blocking software, the IRS maintained or had the ability to maintain information to actively monitor Internet use by employees. The IRS telecommunications infrastructure has most IRS Internet traffic flowing through the Treasury firewall⁷ located at an IRS facility. The firewall records all Internet traffic information on automated logs. In addition, the blocking software used to restrict inappropriate web sites generates an entry to the firewall logs that contains information on blocked web sites.

The IRS did not review the firewall logs to identify inappropriate web sites being accessed. In the previous Internet use example where we found 1 workstation was accessing primarily sexually explicit web sites, the blocking software prevented over 7,700 (4.5 percent) of the 172,000 Internet web objects from being accessed. On 1 day, the blocking software blocked accesses to over 1,000 sexually explicit web objects.

The IRS also had at least five proxy servers⁸ throughout the country. These proxy servers acted as funneling

⁷ A firewall is a computer component with a set of programs that protects internal computer resources from outside (Internet) sources.

⁸ A proxy server is an intermediate computer between a group of employee computers and the firewall (Internet). At the time of our review, IRS Information Systems did not definitively know the number of proxy servers in the IRS.

Employees' Extensive Personal Use of the Internet Should Be Controlled

points to the firewall for Internet accesses. The proxy servers automatically generate logs to track all Internet traffic coming into and going out of the proxy server. As a general security function of proxy servers, all traffic leaving the proxy server will have the proxy server's identification number, not the originating computer's identification number. As such, the logs become important for the purpose of tracing Internet traffic back to its originating source computer.

However, these logs were not retained. By not retaining these proxy server logs, the IRS cannot identify employees requesting access to a particular web site. This impedes management's ability to evaluate Internet activity and identify specific workstations, as well as that of any organization needing this information (e.g., labor relations, investigative, or audit functions). During our review, the OI was unable to obtain the proxy server logs to assist in an investigation because the logs were not maintained.

We have two final notes on Internet use that may be affected by current events within the IRS and federal government. All the conditions and effects cited in this report will take on greater meaning (1) when the IRS expands Internet capabilities to the rest of its 97,800 employees, and (2) if the IRS considers approving a "limited personal use" Internet policy. The Executive Branch Chief Information Officer Council has issued a proposal on allowing federal employees to use the Internet at government facilities before and after their workday and at lunchtime. However, in considering whether to adopt this policy, the IRS should consider that personal use of the Internet by employees within one time zone during "off-duty" hours might affect the telecommunications capacity available for business use of the Internet or electronic mail in another time zone.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Recommendations

The IRS should implement procedures and controls to enforce its Policy on Electronic Communications. The following actions will specifically address the Internet use responsibilities.

1. The Chief Information Officer (CIO) should continue using the Internet blocking software and ensure the timely annual procurement of the software licensing agreement to receive timely updates to the blocking criteria list, starting with the year 2001.
2. The CIO should mandate that all Internet-related activity logs from the IRS firewall and proxy servers are retained and periodically reviewed to identify inappropriate accesses.
3. The CIO should augment the vendor's blocking criteria list with other known inappropriate sites identified during monitoring efforts or from referrals. Based on our review, external streaming media web sites should be blocked from employee access until the IRS Telecommunications Branch can fully evaluate its impact on bandwidth and ensure its use will not hinder other business telecommunications traffic.
4. The CIO should consider the impact on IRS resources prior to deciding to implement a "limited personal use" Internet policy.

Management's Response: Management generally agreed with the findings and their response is included as Appendix IV. Management agreed to focus on using commercially available blocking software, educating employees and managers on employee productivity issues, and performing random checks on usage. However, management's response was incomplete because it did not identify the specific corrective actions to be taken, the responsible officials, and the implementation dates. We will follow up to obtain this additional required information.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Conclusion

Granting employees access to the Internet can be an effective business tool. Almost 16,000 of the 97,800 IRS employees currently have access to the Internet, and there is tremendous potential for expansion of this tool. Misuse of the Internet, however, can diminish productivity and increase telecommunications demands. To minimize the misuse of the Internet, management must take actions to increase employees' awareness of the impact of misuse, block inappropriate sites, and periodically monitor Internet activity.

Employees' Extensive Personal Use of the Internet Should Be Controlled

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) complied with the Department of the Treasury policy on the use of the Internet.

- I. We identified the IRS' current Internet use policy and determined whether the IRS had an effective process or control to measure and monitor adherence to the policy.
 - A. Identified the contents and current status of the IRS' own policy over Internet use and access, as well as the Treasury-wide and government-wide policies on Internet use that affect the IRS.
 - B. Diagramed the telecommunications flow from when an employee requests access to the Internet/World Wide Web to when the employee receives the requested information from the web site. We identified the use of proxy servers and firewalls in the process and existing policies associated with this process.
 - C. Determined if the IRS had procedures to monitor Internet access activities. We identified any obstacles the IRS had encountered regarding the monitoring of Internet use.
 - D. Determined if the IRS used or considered using web site filters or blocking software to restrict the types of Internet web sites that can be accessed. If filtering or blocking were used, we evaluated the settings and configurations to determine whether the control worked as intended.
 - E. Interviewed personnel from the IRS Offices of Labor Relations and Information Systems Data Security to identify instances and occurrences of violations of Internet policies and determined the impact of the violation.
- II. We profiled IRS employee Internet use to identify what types of web sites were accessed and how much time was spent on the Internet.
 - A. Obtained information on all available Internet accesses from IRS workstations that flow through the accredited Treasury firewall at an IRS facility for January and February 2000. We also obtained data on Internet traffic from IRS workstations through the accredited firewall at the Department of the Treasury facility. Because these data were received well after we received the IRS firewall data and the volume consisted of 5 percent of the total IRS Internet traffic, we decided not to include this information in our review.

Employees' Extensive Personal Use of the Internet Should Be Controlled

- B. Selected 7 days from the 2-month period of data, with 1 day from each week and each day of the week represented – January 10 (Monday), January 21 (Friday), January 25 (Tuesday), February 3 (Thursday), February 16 (Wednesday), February 26 (Saturday), and February 27 (Sunday). We identified the following days during our population period where all or partial data on Internet accesses were not available for review: January 1 to 9 and 14; February 4 to 15, 17, 19, 20, and 21.
- C. For the 7 days, categorized each of the 16,781,674 web object records accessed by the object's destination web site, ranked the web sites based on highest volume of duration (transmission time), and conducted further review on the top 200 web sites accessed by employees for each day.
- D. For the top 200 web sites accessed by employees for the 7 days, stratified the 10,042,389 web object records into the following web site categories. We used content filtering programs to identify into which category each record fell. Because each record represented a web object,¹ we could not identify the number of Internet accesses made since one access could represent several objects.
- Business: IRS case-related, U.S. government, information technology, travel, and employee personnel support.
 - Non-Business: financial, Internet Service Provider chat room and electronic mail, sexually explicit, sports, shopping, and gambling.
 - Business/Non-Business: news outlets, streaming media, and search requests.
- In each category, any object that did not fit into the above categories was counted into the miscellaneous categories.
- E. For the Business/Non-Business categories, conducted additional research, such as database filtering, web object analysis, and re-creating the accesses, to determine the web objects' business application.
- F. Quantified the objects in terms of transmission duration in seconds. Transmission duration is the time from when an employee sends an Internet web site access request to when the electronic information is delivered to the employee.
- G. Conducted Internet research to identify and/or confirm the web site being visited by the employees for the top 200 sites and to determine whether the web site's contents were consistent with the performance of IRS official duties.

¹ A web object represents a single file on a web site. The file could be a web page itself or any object on a web page, such as a picture or banner.

Employees' Extensive Personal Use of the Internet Should Be Controlled

- III. We evaluated the impact of employee Internet use on telecommunications capacity and resources.
- A. Interviewed IRS Information Systems Telecommunications personnel to identify data flow between workstations, proxy servers, and firewalls in terms of telecommunications resources and monitoring efforts on telecommunications traffic and activity.
 - B. Obtained statistical information kept regarding telecommunications usage from Internet activities, as they related to the overall telecommunications traffic.
 - C. Identified how the IRS evaluates telecommunications needs and resources required to support IRS telecommunications activities, particularly from Internet accesses. We determined if plans exist to increase or decrease telecommunications resources due to needs.
 - D. Identified the impact of the transmission duration of the web objects on telecommunications capacity for our 7-day sample.

**Employees' Extensive Personal Use of the Internet
Should Be Controlled**

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Harry Dougherty, Senior Auditor
Louis Lee, Senior Auditor
Larry Reimer, Senior Auditor

**Employees' Extensive Personal Use of the Internet
Should Be Controlled**

Appendix III

Report Distribution List

Deputy Commissioner Operations C:DO
Chief Information Officer IS
Deputy Chief Information Officer, Operations IS
Director, Telecommunications IS:T
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis M:O
The Office of the Chief Counsel CC
The Office of Management Controls CFO:A:M
National Taxpayer Advocate TA
Audit Liaison: Information Systems Audit Assessment and Control IS

Employees' Extensive Personal Use of the Internet
Should Be Controlled

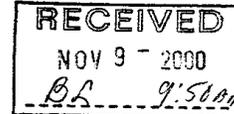
Appendix IV

Management's Response to the Draft Report



DEPUTY COMMISSIONER

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



November 8, 2000

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR
TAX ADMINISTRATION

FROM: Bob Wenzel 
Deputy Commissioner

SUBJECT: Response to Draft Audit Report: Employee's Extensive
Personal Use of the Internet Should be Controlled
(Audit No. 200020030)

This letter provides my comments on your draft report, *Employee's Extensive Personal Use of the Internet Should be Controlled*. Thank you for the opportunity to comment. In brief, you are correct in recommending that the IRS should improve enforcement of its policy on electronic communications and, after a delay caused in part by protracted labor negotiations, we are doing just that. Unfortunately, this is a complex problem that has many facets and raises a number of critical issues that we are focused on solving. Let me address each of these issues in turn.

First, I cannot over emphasize my commitment, or that of the IRS Senior Leadership Team, to ensuring our employees use the Internet properly. Your recommendation that we do more to educate our employees about the policy and take steps to enforce it is right on point.

Now that we have a negotiated Internet policy, we are taking steps to implement it. Since December 1999, we have deployed updated software to block inappropriate sites and we are developing a far-reaching communications effort to ensure that our workforce understands the policy and what is expected of them. We are also beginning an analysis of other monitoring strategies we should adopt to make sure that the policy is being followed.

It is also important to point out that our current policy may soon change. In fact, the Treasury Department has recently approved a modification that provides for limited personal Internet use. This modification, if adopted by the IRS, is more flexible than our current policy. We must now evaluate this modification and consider its impact on our employees including negotiating its implementation with NTEU.

Employees' Extensive Personal Use of the Internet Should Be Controlled

2

Next, I wish to comment that tracking Internet usage and determining if the usage is for business or personal use is a very difficult task. We use technology that permits us to establish an access audit trail but matching specific usage to a specific employee is not a straightforward process. In addition, it is extremely difficult to determine if the access is for personal or business usage. For example, an assumption that financial web sites (e.g. Banking and Stock Trading) constitutes personal usage is sometimes difficult to make since many of our personnel might visit these same sites in their official capacities.

Since we have very limited resources to address this need for oversight and control we will be much better serviced by focusing our actions as follows:

- Enforce the use of commercially available blocking software
- Improve employee/manager education and focus any issues related to employee productivity at this level
- Perform random checks on usage.

This will allow the IRS to do a better job of ensuring its employees know and follow our policy guidelines. As I mentioned earlier, we are committed to making this happen. I was very disturbed that you uncovered one case in which an employee had accessed a sexually explicit web site. Let me be clear on this point. I will not tolerate this kind of activity by an IRS employee and I will take immediate action to address this type of wrongdoing. I look forward to the results of your investigation on this case and on the others you encountered during your review.

Finally, I was heartened by your recommendation that the CIO should consider resource impacts of Internet policy changes. I believe that this approach makes good management sense. In fact, within the government-wide limits, we intend to review private-sector best practices and approaches to making further modifications to our Internet use policy.

I would be happy to discuss the report and our response with you. I can be reached at (202) 622-4255. In addition, Paul Cosgrave, our Chief Information Officer (202) 622-6800 and Alfred Whitley, Director, Telecommunications, (202) 283-0990 are also available.