

September 2, 2003

MEMORANDUM TO: William D. Travers
Executive Director for Operations

FROM: Stephen D. Dingbaum/RA/
Assistant Inspector General for Audits

SUBJECT: MEMORANDUM REPORT: FOLLOW-UP REVIEW OF
NRC'S INTERNET USAGE (OIG-03-A-21)

In October 2001, the Office of the Inspector General (OIG) reported that based on an assessment over an 8-day period in June 2001, 52 percent of agency employee Internet activity was for personal use.¹ Approximately 5 percent of the personal use was in direct violation of NRC policy and was referred to the OIG investigative staff for further review. OIG reported that because of the amount of personal use and the occurrences of prohibited use, the Nuclear Regulatory Commission (NRC) needed to enforce its policy for personal Internet usage. The report made five recommendations to the Executive Director for Operations to develop, issue, and communicate a revised Internet usage policy and to restrict prohibited Internet activity. The agency has implemented corrective actions in response to the recommendations in the October 2001 audit report. The recommendations and the corrective actions appear on pages three through six of this report.

OIG has completed a follow-up audit on Internet use to determine the status of the recommendations made in the October 2001 audit report, the amount of employee personal Internet use, and the frequency of prohibited Internet activity. The audit was intended to provide a general characterization of NRC's Internet use. A comparison of the January 2003 Internet data to the June 2001 data showed that personal use of the Internet remained virtually the same, while prohibited activity (e.g., visiting sexually explicit Web sites) decreased. Specifically, 51 percent of NRC employee Internet activity was for personal use in 2003, compared to 52 percent in 2001. However, prohibited activity decreased to less than 1 percent in 2003 from 5 percent in 2001. Because the total amount of personal use remains over 50 percent, this report contains two recommendations to manage personal use of the Internet at NRC.

¹ Report OIG-02-A-01 entitled *Use of the Internet at NRC*, dated October 15, 2001.

NRC Policy

Management Directive (MD) 2.7, *Personal Use of Information Technology*, defines acceptable conditions for NRC employees' personal use of information technology (IT). MD 2.7 was issued on the basis of recommendations from the Federal Chief Information Officer Council's Government-wide policy guidance, "*Limited Personal Use of Government Equipment Including Information Technology*," which provides a backdrop of conditions for an agency to consider when developing a personal use policy for Government office resources. The policy and guidance in MD 2.7 states that personal use of the Internet is acceptable² when such use:

- Involves minimal or no additional expense to the Government.
- Is performed during employee non-work time.
- Does not interfere with NRC's mission or operation.
- Does not violate Federal Government Standards of Ethical Conduct.
- Is not otherwise prohibited by law.

PURPOSE

The objectives of this follow-up audit were to:

1. Review the implementation of corrective actions taken since October 2001 to strengthen management controls over employee personal use of the Internet.
2. Characterize NRC employees' use of the Internet to determine whether the use was in compliance with NRC policy.

² MD 2.7 states that the policy and guidance applies to all NRC employees, including Special Government Employees. NRC contractors are prohibited from personal use of agency information technology.

RESULTS

Agency actions taken as a result of the recommendations from the previous OIG report have greatly reduced the amount of prohibited access to Web sites. Based on a 1-week period in January 2003, OIG determined that 51 percent of employee Internet use was for personal use. Prohibited use however declined from 5 percent to less than 1 percent as a result of the agency's blocking of inappropriate Web sites. Specifics on these matters are described in the following sections.

Implementation of Corrective Actions

OIG's October 2001 audit report on Internet use made five recommendations to the Executive Director for Operations to help strengthen management controls over the amount of personal use and to restrict prohibited Internet activity.

- Initiate monitoring of Internet activity.
- Review and clarify MD 2.7 to address Internet activity not currently covered, such as Visual Basic Script file type downloads.
- Revise NRC Management Directives, as appropriate, to ensure NRC's Internet use policy covers persons other than NRC employees who use NRC computers to access the Internet.
- Restrict prohibited Internet activity using software or other means.
- Issue a Yellow Announcement, or other appropriate communication, advising employees and other affected users of the agency's revised policy and emphasizing that management will not tolerate prohibited activity.

The agency took the following actions in response to these recommendations.

Initiate monitoring of Internet activity

The Office of the Chief Information Officer (OCIO) monitors Internet activity monthly using a software product that basically shows a trend analysis of Internet use for the agency. This software is not used to monitor individual use, but rather provides information such as general agency statistics, the most popular sites visited, activity levels for the different time periods, and other information.

OCIO recognizes its duty to help ensure the integrity of the agency by not only monitoring but also by providing tools to assist NRC managers in evaluating staff use of the Internet.

Review and clarify Management Directive 2.7 to address Internet activity not currently covered, such as Visual Basic Script file type downloads

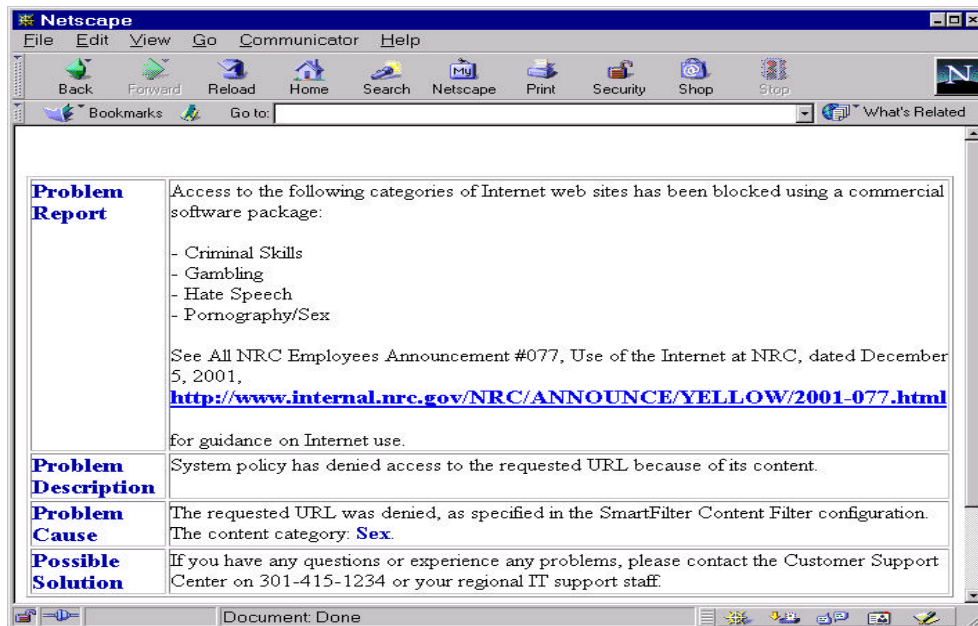
OCIO examined MD 2.7 and found it adequate as written with respect to personal use by NRC employees. MD 2.7 states that personal use of agency IT is a privilege, not a right, and employees should not have the expectation of privacy while using agency IT systems. By using agency IT systems, employees acknowledge their consent to disclosing the contents of any files or information maintained in the systems.

Revise NRC Management Directives, as appropriate, to ensure NRC's Internet use policy covers persons other than NRC employees who use NRC computers to access the Internet

In response to the OIG finding that contractors used the Internet inappropriately, NRC issued a new procurement instruction. This instruction reflects MD 2.7's prohibition of personal use of agency information technology by contractors. The Division of Contracts and Property Management (DCPM) *Instruction 02-01*, issued March 4, 2002, specifically prohibits personal use of IT equipment by contractors. *DCPM Instruction 02-01* states that the contractor must be held responsible for monitoring its employees, consultants, and subcontractors to ensure that NRC-furnished IT equipment and/or IT access is not used for personal activities, misused, or used without proper authorization. To implement this policy, NRC's Division of Contracts requires all solicitations, contracts, or delivery orders that allow contractor staff access to NRC IT equipment and services to include the clause, "*Appropriate Use of Government Furnished Information Technology (IT) Equipment and/or IT Services/Access.*"

Restrict prohibited Internet activity using software or other means

In November 2002, OCIO began using software that places a filter to block inappropriate Web sites. When such a site is accessed, the network displays a message explaining that the site is blocked and why it is inappropriate. A sample picture of the message is displayed below.



Issue a Yellow Announcement, or other appropriate communication, advising employees and other affected users of the agency’s revised policy and emphasizing that management will not tolerate prohibited activity

A Yellow Announcement was issued in December 2001 and in February 2003 to remind employees of NRC’s Internet limited personal use policy. It stated that NRC employees must exercise common sense, good judgment, and propriety in the use of this valuable resource. The announcement reminded the staff that NRC allows employees to access the Internet for limited personal use when such use involves minimal or no additional expense to the Government, is performed on the employee’s non-work time, does not violate the Standards of Ethical Conduct for Employees, and is not otherwise prohibited by law.

Characterization of Current Internet Use

During a 1-week period in January 2003, 51 percent of NRC employee Internet activity appeared to be for personal use. Although each individual accessing the Internet may not be a problem, the composite total of personal Internet use is over 50 percent. NRC currently does not employ a management tool that enables individual use to be routinely monitored. Thus, the agency could experience a public relations issue in the future if the public perceives this rate as excessive.

Internet use is largely personal

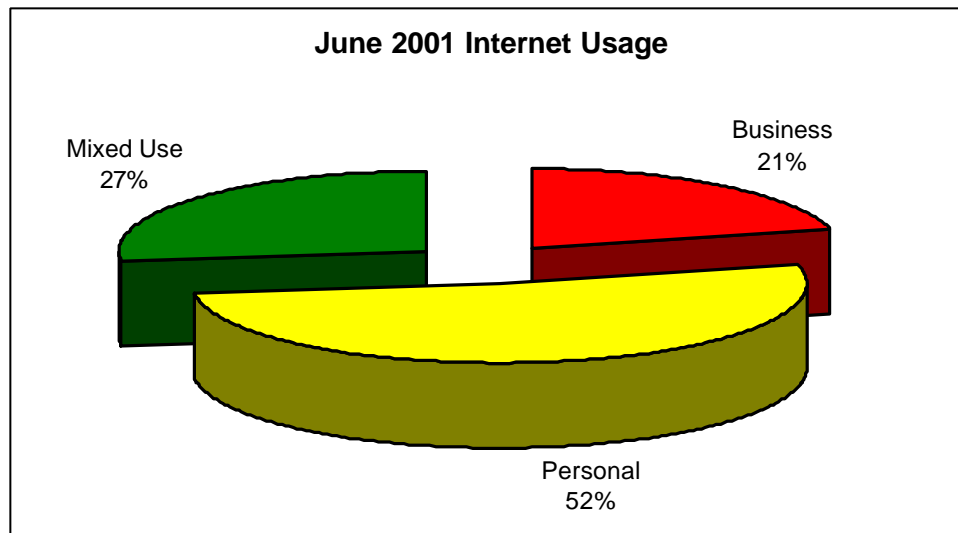
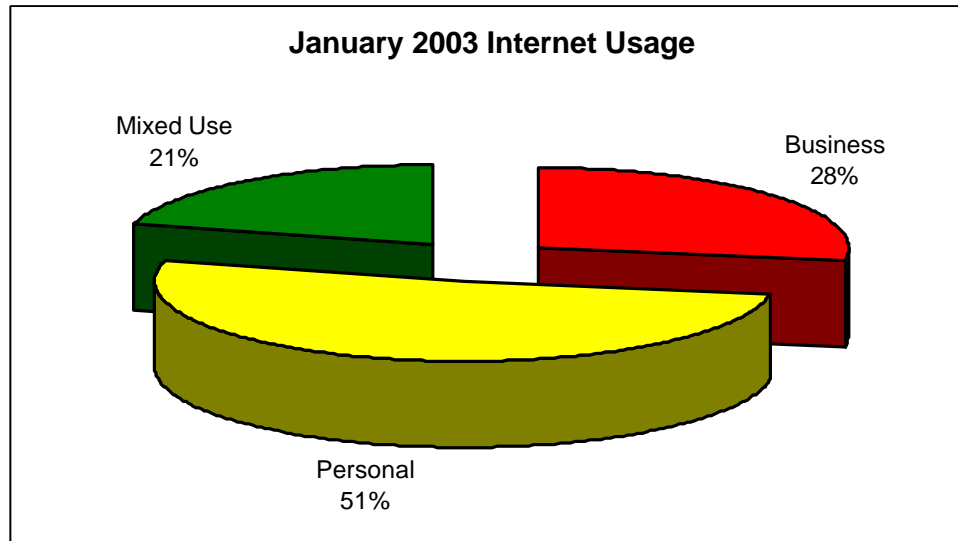
As part of its assessment of employee³ Internet use for a 1-week period in January 2003, OIG analyzed accessed Web sites that represented about 75 percent of all sites visited for that week.

To analyze Internet use, OIG used data that provided the volume of information transferred⁴ to the employees' computers. Internet activity was categorized as business or personal. In addition, some Web sites could have been accessed for either business or personal reasons and were therefore categorized as mixed use in this report. Examples of mixed use are news sites and search engines such as www.google.com. The analysis did not break out non-working hours from working hours. In addition, the analysis did not determine actual time spent using the Internet.

³ Employee use included use of the Internet by NRC contractors. OIG included contractor use because contractors are accessing the Internet for personal use.

⁴ This information transfer is referred to in this report as activity and indicates the actual number of bytes of information that were transferred to an employee's computer from the logs. The logs do not provide duration or the amount of time the site is in use.

Comparison of Internet Use in 2003 and 2001⁵



⁵ The 2001 analysis was based on the number of bytes of information transferred to an employee's computer over an 8-day period in June 2001, while the 2003 data was based on a 1-week period in January 2003. The 2001 analysis was based on a review of the logs similar to those used for the 2003 analysis.

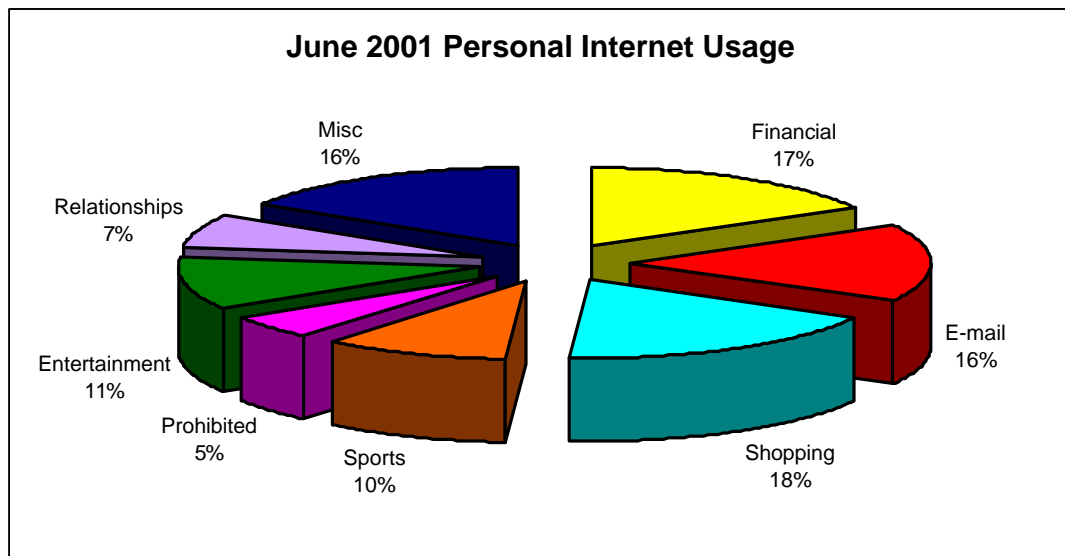
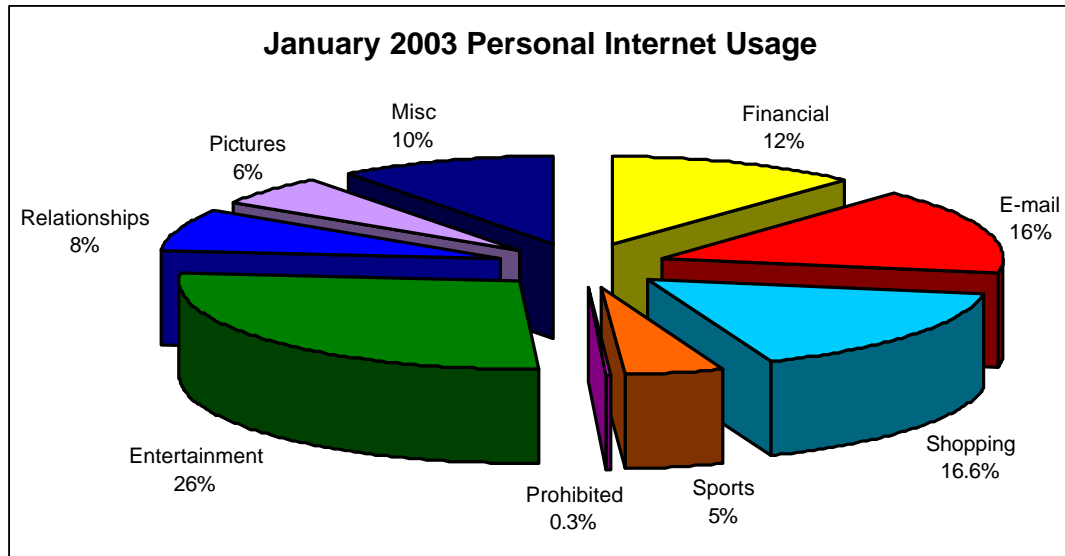
Local and national news Web sites such as the Washington Post, CNN, and USA Today dominate the mixed use category. Those Web sites were not placed in either the business or personal use category because they can be used for both reasons.

The agency does not monitor Internet use by individuals. While each individual instance of Internet use could well be within the agency's de minimis use policy, the total personal use is so high that it leaves NRC vulnerable to criticism for excessive employee time on the Internet.

Prohibited use of the Internet

A further breakdown of the personal Internet use in 2003 and 2001 is shown in the following charts which detail the wide variety of Web sites that employees accessed. The individuals who abused the usage policy by accessing prohibited Web sites, including sexually explicit, gambling, and hate sites, were referred to OIG's investigative staff. However, prohibited use of the Internet decreased from 5 percent in 2001 to less than 1 percent in January 2003. Thus, the filtering software blocking prohibited Web sites is effective at decreasing this kind of activity. However, some instances still occur when individuals visit locations where filtering does not work, such as e-mail or instant messaging. Subsequent to our fieldwork, management officials stated that the issue of bypassing the content filtering by using instant messaging has been resolved by blocking instant messaging capability for the agency. Visits to these types of Web sites are significant because the site contents may be offensive to others and could lead to potential legal liabilities for the agency. NRC needs to continue to send a strong message about inappropriate Internet use.

Internet Use in 2003 and 2001



Conclusion

During non-work time, NRC employees are allowed to use information technology resources, including the Internet, for personal reasons when that use is in accordance with NRC's limited use policy. More agency action is needed to enforce contractor and employee personal Internet usage requirements.

Because personal use is high as compared to the amount of overall Internet activity, NRC could suffer adverse publicity if the perception is that employees are spending excessive time pursuing personal interests at the expense of their work responsibilities.

RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Provide management tools that will assist NRC managers and supervisors to evaluate Internet usage within their organization to (1) determine if their organizations are adhering to the agency's de minimis Internet use policy and (2) take corrective actions where necessary.
2. Develop and implement an approach to periodically make NRC managers aware of their responsibilities regarding minimal employee use of the Internet.

AGENCY COMMENTS

On August 4, 2003, OIG discussed its draft report with agency senior executives who generally agreed with the report recommendations. This final report incorporates agency comments, where appropriate.

SCOPE AND METHODOLOGY

The scope of this audit was generally limited to analysis and evaluation of the Internet use during a 1-week period in January 2003. OIG reviewed NRC's current Internet usage policy. OIG also met with NRC officials in NRC's OCIO. To perform this review and build a profile of employee usage, OIG obtained firewall logs from the agency for the period under review. These firewalls contain logs of Web sites visited; the breakdown used for OIG's analysis looked at Web pages visited and did not take into consideration instant messaging and chat rooms. The 1-week period that OIG selected occurred slightly over 1 month after the filtering software was in place to ensure that data analysis would take into consideration the filtering of inappropriate Web sites. OIG determined the amount of information transferred from each Web site. This information transfer (termed activity) indicates the actual number of bytes of information that were transferred to an employee's computer through the proxy server. OIG analyzed

about 75 percent of all agency Internet use for a 1-week period by reviewing 1,400 Web sites accessed in January 2003.

OIG trimmed each full Internet address shown in the firewall log to a base address and reviewed the material at the address to evaluate its probable use. Based generally on the material at the Web page accessed, OIG determined whether the use was business, personal, or a combination of personal and business reasons. OIG could not determine whether employees were spending inappropriate amounts of time using the Internet for personal reasons because firewall logs provide insufficient information to make such a determination.

The audit was conducted from January through May 2003 in accordance with generally accepted Government auditing standards and included a review of management controls related to the objectives of the audit.

The major contributors to this report were Beth Serepca, Audit Manager, and Rebecca Underhill, Management Analyst.

cc: Chairman Diaz
Commissioner McGaffigan
Commissioner Merrifield
William Dean, OEDO

Document Location: WORD DOC\G:\Audit\03-a-21\Final Report.doc

Distribution

OIG Chron

AIGA Chron

File: 03-a-21

RUnderhill

BSerepca

OIG	OIG	OIG	OIG	OIG	OIG
RUnderhill	BSerepca	TLipuma	SDingbaum	DLee	Hbell
08/ /03	08/ /03	08/ /03	03/ /03	03/ /03	03/ /03

Official File Copy