



DEPARTMENT OF THE INTERIOR Office of Inspector General

Excessive Indulgences

Personal Use of the Internet at the Department of the Interior





United States Department of the Interior

Office of Inspector General

Washington, D.C. 20240

September 18, 2006

Memorandum

To: Dirk Kempthorne
Secretary

From: Earl E. Devaney
Inspector General

Subject: Personal Use of the Internet at the Department of the Interior
(No. Y-EV-MOA-0002-2006)

This memorandum transmits our report detailing personal use of the Internet at the Department of the Interior. We conducted this review to determine whether the Department has implemented effective controls to ensure compliance with Internet usage policies. Our review concentrated on Internet use involving sexually explicit and gambling websites, which are expressly prohibited, along with gaming and auction websites, which are typically time consuming and thus interfere with employee productivity.

We discovered that computer users at the Department have continued to access sexually explicit and gambling websites due to the lack of consistency in Department controls over Internet use. While not specifically prohibited, we also discovered that computer users spent significant time at Internet auction and on-line gaming websites, costing an estimated 104,221 hours in potential lost productivity over the course of a year.

Misuse of Internet resources exposes the Department to legal liability, degrades system resources, and compromises system integrity. Without strong and effective controls, we believe that this activity will continue and possibly increase. Our report contains recommendations for improving Department control of Internet use and holding those who violate established Internet policies accountable for their actions.

If you have any questions about this report, please do not hesitate to contact me at (202) 208-6619.



Introduction

DOI promotes Internet use that enables employees to perform Departmental missions and encourages its employees, volunteers, and contractor personnel to develop Internet skills and knowledge. With Internet access available to the majority of the 80,000 employees, along with numerous volunteers and contractors, proper controls are required to prevent misuse and improper access to prohibited websites.

The Office of Inspector General (OIG) conducted a limited-scope review to determine whether the Department has effective controls in place to ensure compliance with agency policies on Internet usage. Our review primarily focused on whether DOI computer users are complying with directives restricting access to sexually explicit, gambling, gaming, and auction websites. We concentrated on Internet use involving sexually explicit and gambling sites as they clearly constitute an egregious violation of DOI policy; on-line gaming and auction sites were included as recognized sites that would typically be non-work related and time consuming, thus interfering with employee work production. We did not examine visits to all other forms of non-work related websites that could not as readily be identified as constituting inappropriate use of the Internet or requiring extended viewing periods.

Sexually Explicit & Gambling Sites
Clearly constitute an egregious violation of DOI policy
On-line Games & Auction Sites
Non-work related, time consuming, interfere with employee work productivity

In addition, we reviewed Department efforts to identify, monitor, and prevent access to sexually explicit and gambling websites along with actions taken by management to hold employees accountable for non-compliance with established Internet use policies. We also reviewed OIG investigative files regarding Internet misuse.

Our review was conducted in accordance with the President's Council on Integrity and Efficiency Quality Standards for Inspections. To accomplish our review, we interviewed key DOI personnel and examined DOI and Bureau policies governing the use of the Internet. We collected Internet usage logs from six Bureaus and offices (Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Minerals Management Service (MMS), National Park Service (NPS), Office of Surface Mining (OSM), and US Geological Survey (USGS)) for a specific 7-day period. We then extracted and analyzed log entries, which are generated each time a computer accesses a website, using widely-accepted lists of keywords and popular Internet addresses for each category. These lists were not exhaustive, as website addresses can frequently change. Both Fish and Wildlife Service (FWS) and National Business Center (NBC) were unable to provide the data we requested. The Bureau of Indian Affairs (BIA) was not included in our review because of the Cobell Court's injunction against Internet use by BIA.



Access to Prohibited/Inappropriate Web Sites

Our review of 1 week of computer use logs revealed over 4,732 log entries relating to sexually explicit and gambling websites that had been accessed by Department computers. We estimated that this activity accounted for over 24 hours of Internet use during our sample period; however, our analysis did not include a review of email or other means of transferring prohibited material.

Every Year...

Employees Accessing Auction and
Game Sites are Potentially Costing the
Department of the Interior...

\$2,027,887.68
per year

\$38,997.84
per week



More alarming was our finding regarding access to on-line game and auction websites: we discovered over 1,000,000 log entries where 7,763 Department computer users spent over 2,004 hours accessing game and auction sites during

that same week. Over a period of 1 year, these veritable shopping and gaming binges could account for 104,221 hours of lost productivity.

We believe that our estimates of inappropriate use activity are conservative, particularly the amount of time spent at pornographic and/or sexually explicit websites.

While we did not focus on individual employee Internet usage, we did uncover noteworthy cases of egregious usage in each of the Bureaus. For example, we discovered:

- A number of computers accessed sexually explicit websites for approximately 30 minutes to nearly 1 hour;
- One computer had 2,369 computer log entries at two Internet game sites for approximately 14 hours;
- 406 computer log entries indicating another computer accessed an Internet game for approximately 12 hours;
- 2,949 computer log entries indicating a third computer accessed an Internet game site for nearly 10 hours; and,
- 12,597 computer log entries indicating a fourth computer accessed an Internet auction for nearly 8 hours.

In a review of OIG investigative files, we found that our investigators routinely discover evidence that employees access sexually explicit websites.

Pornography, and in some cases child pornography, have been discovered during forensic examinations of Department computers. Often, the discovery of pornography is incidental to the purpose of the forensic examination. For example:

- A DOI employee was sentenced to 8 years in prison for possession of approximately 30,000 images of child pornography, which was discovered

One full-time employee normally works 2,080 hours per year.

Our findings suggest that the equivalent of 50 FTEs spend all their work hours surfing Internet on-line game and auction websites over the course of a year.

on his government computer during an examination for a computer virus.



- We discovered more than 2,000 pornographic images, including child pornography, after two other DOI employees' computers were examined for computer viruses. Each employee was subsequently prosecuted and sentenced to 21 months of incarceration.
- Another employee was sentenced to 10 months of imprisonment and ordered to pay \$25,000 in restitution to the government for the time he spent surfing pornographic websites, which we uncovered during an investigation of false time and attendance entries.

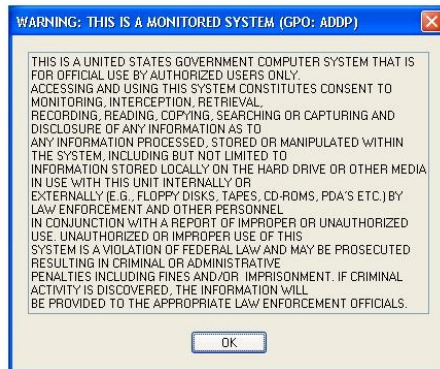
Accessing sexually explicit websites, in particular, can often compromise, degrade, or paralyze computer systems through the introduction of computer viruses or other malicious software frequently contracted from these websites. Sexually explicit websites can also contribute to creating a hostile work environment, exposing the Department to increased liability.



Policies and Preventive Measures

We found a myriad of Department, Bureau, and Regional-level policies governing access to and use of the Internet by DOI computer users. Generally, these policies are sufficiently detailed to explain the proper use of the Internet. In many cases, the Bureau's policy mirrors the Department's policy.

Additional guidance for Department Internet users is provided through annual information systems security training, which is required for every DOI computer user. Moreover, users are notified of restrictions and penalties for unauthorized



use of DOI computer systems through warning banners that appear on the computer screen during initial sign-on to the system. When a Bureau uses Internet monitoring tools, a secondary warning banner also notifies computer users who attempt to access prohibited Internet websites that the site has been blocked.

While the Department currently has no system-wide infrastructure that provides Internet monitoring and blocking capabilities that would enable computer users to be routinely and easily monitored, there are plans to provide such capabilities in the Department's Enterprise Services Network (ESN) in the future.

Simplified, the ESN provides access to the Internet through a centralized network of five shared "gateways" across the country. The majority of DOI computer users access the Internet through these "gateways." We were told that the DOI Office of Chief Information Officer (OCIO) recently tested and selected an Internet monitoring and blocking tool for the ESN. Due to additional testing requirements and a yet-to-be determined delivery date for the necessary hardware, the ESN program manager was unable to tell us when that tool will actually be installed.

Since the OCIO will ultimately control the monitoring and blocking of inappropriate Internet websites through the ESN, it is attempting to develop standardized criteria and definitions used to block inappropriate websites. According to the OCIO, attempts to gain Bureau participation and assistance in developing this information have been met with resistance and indifference. Similarly, we were told that the Solicitor's Office has failed to respond to an OCIO request for guidance. Consequently, a unified, coherent and effective methodology for detecting, monitoring, blocking, and referring inappropriate, illegal, and prohibited Internet usage for potential disciplinary action has yet to be developed.

We found that most Bureaus do not routinely review Internet log files to detect inappropriate, illegal, and/or prohibited use similar to the methodology we employed. In the absence of a Department-wide monitoring program, four Bureaus (BLM, OSM, BOR, and FWS) have implemented and are using Internet website monitoring and blocking software programs to varying degrees and with some success. BLM has implemented the most proactive methodology to block access to inappropriate websites and utilizes a full-time contractor to monitor Internet usage activity.

Although OSM uses an Internet monitoring and blocking software program, one OSM official told us that they do not routinely review and monitor Internet usage data, rendering the system useless for any real proactive measures. It appears that, at OSM, Internet usage reports are only generated and analyzed when specific requests are received from a supervisor who believes that an OSM employee is violating OSM policy.

The value of BOR's Internet website monitoring and blocking software is questionable. We discovered a volume of continuing inappropriate Internet occurrences, which suggests that some employees are able to circumvent controls used by the software program. We found over 1,530 log entries for 148 separate BOR computers that had succeeded in accessing sexually explicit websites.

We were told that FWS Internet monitoring and blocking software became operational recently, on August 7, 2006.

We found the use of the web filtering tools provide some level of protection for the Bureaus that used them, but users were still able to gain access to prohibited sites despite the employment of web filtering software. In a final spot check in August 2006, we attempted access to eight known sexually explicit and gambling websites on each system. We were able to access sexually explicit photographs through BLM, FWS, and OSM computer systems, but not through the BOR computer system. Additionally, we were able to access gambling sites using BOR, FWS, and OSM computers, but not through the BLM computer system. Based on our findings, we believe that the Department and Bureaus would do well to not be lulled into a false sense of security that these filtering tools provide a significant level of protection. Instead, reports generated by these filtering

tools should be routinely reviewed to promptly identify prohibited activity and close the gap in the software capabilities.

USGS, MMS, NBC, and NPS do not currently have any type of Internet monitoring or blocking software programs in place. USGS and NPS officials told us they are researching software to monitor Internet use and block inappropriate websites. Officials at MMS and NBC told us that they currently do not have any ability to monitor Internet usage and will rely upon ESN for monitoring Internet usage once ESN provides that service. An NBC manager told us that she uses “management by walking around” to monitor and control Internet usage due to the absence of a formal monitoring tool.



Disciplinary Action Taken

Bureau officials reported there have been only 177 disciplinary actions imposed on DOI computer users for inappropriate Internet use since 1999. We discovered that 112 of the 177 (63%) disciplinary actions were for accessing pornographic or sexually explicit websites. Disciplinary action was imposed on employees with tenure ranging from less than 1 year to 38 years of service. Employee grade levels ranged from GS-1 to a GS-15. Twenty of the employees disciplined were in supervisory positions.



Reported disciplinary actions averaged 25 per year over the past 7 years among eight Bureaus. The low number of disciplinary actions reportedly taken against employees who had violated Department and Bureau Internet Acceptable Use Policies compared to the thousands of hits we found indicating user activity at inappropriate sites suggests that employees are not being held accountable for non-work related and inappropriate use of the Internet.



Conclusion and Recommendations

Current Department, Bureau, and Regional efforts to prevent, deter, and detect Internet access to inappropriate websites are inconsistent and must be improved. Despite software filtering programs, training, and policies, computer users are still able to exploit the lack of consistency in Department controls over Internet use to access prohibited material. This misuse results in lost productivity, exposes the Department to legal liability, degrades system resources, and compromises system integrity.

Recommendation #1

Department and Bureau officials should develop a unified methodology to address inappropriate and/or prohibited Internet use on a Department-wide basis. This would include proactive efforts by managers to identify and respond to instances of inappropriate Internet use using properly configured software and education programs.

Recommendation #2

Those who violate established Internet use policies should be held accountable for their actions. We believe that predictable and persistent disciplinary action against violators will significantly influence abusive Internet use practices and further reduce the cost of lost productivity.

How to Report Fraud, Waste, Abuse and Mismanagement

Fraud, waste, and abuse in government are the concern of everyone, Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to departmental or Insular Area programs and operations. You can report allegations to us by:

Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 5341-MIB
1849 C Street, NW
Washington, DC 20240

Phone:

24-Hour Toll Free	800-424-5081
Washington Metro Area	202-208-5300
Hearing Impaired (TTY)	202-208-2420
Fax	202-208-6081
Caribbean Field Office	340-774-8300
Northern Pacific Field Office	916-978-5630*

Internet:

http://www.doiig.gov/form/hotlinecmp_form.php

*Use Western Region Investigations telephone number until further notice



U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW
Washington, DC 20240

www.doi.gov
www.doiig.gov

