United States Nuclear Regulatory Commission

NUREG/BR 0272
Volume 3, Issue 1

June 2002

OIG FRAUD BULLETIN

Use of Information Technology

Did you ever imagine you could walk around a shopping mall and talk on the telephone at the same time? Did you think it would be possible to have a little box attached to your belt that would inform you when someone was trying to call you? Did it ever occur to you that one day you would not have to use five carbons to type a memorandum and not have to rely on your memory for correct spelling? How about using a laptop on an airplane? Remarkable!

Information Technology has rapidly advanced over the last decade and has unlocked new frontiers for education, research, and sharing certain technologies with people all over the world. The Internet is an extremely useful tool that when used properly can make an employee's job much easier.

As beneficial as the appropriate use of the Internet can be, the repercussions for misuse of the Internet by a government employee can be very costly. Certain sites on the Internet can be dangerous and illegal places to visit. Too much personal use can slow down information transfer from the network to other computers. Employee productivity may also be affected by excess personal use of the Internet.

Use of the Internet is a privilege...not a right. Misuse of government Information Technology is a misconduct issue and employees could be the subject of disciplinary action. Accessing sites of a pornographic nature is an example of this type of misconduct.

Be mindful of what appears on the screen of your computer.

Statutes, regulations, NRC Management Directives and policy all provide guidance on the proper and improper use of government equipment. This edition of the OIG Fraud Bulletin is intended to summarize and clarify guidance on the use of Information Technology equipment in the workplace and assist you in the proper use of the Internet and all related government equipment.

Inside this issue:

Special points of interest:

- OIG cases involving pornographic sites
- News Articles on other agencies views of these sites
- Proper Use of NRC IT Equipment
- New ATM Scam you should know about

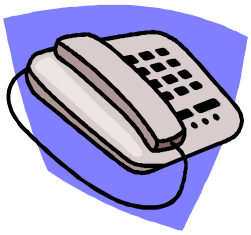
Authorized Uses of Information Technology Equipment for Personal Use

Management Directive 2.7

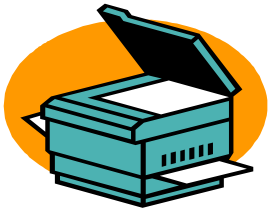
According to Management Directive 2.7, the "NRC is extending the opportunity to its employees to use government property for personal use in an effort to create a more supportive work environment. In this sense, the policy grants a privilege, not a right, to use agency Information Technology for certain non-government purposes."

Use of any NRC Information Technology for personal use is acceptable provided such use involves 1) minimal expense to the government, 2) is performed before or after work or during a lunch period, 3) does not interfere with NRC's mission, 4) does not violate the Standards of Ethical Conduct for Employees of the Executive Branch, and 5) is not prohibited by law.

Equipment use includes personal computers, printers, software, telephones, pagers, facsimile machines, photocopiers, E-mail and the Internet.



Minimal additional expense. An NRC telephone may be used for personal use to call a day care provider, doctor, spouse, dentist, elderly care or other place or person that may not be available after normal work hours. The telephone numbers that are dialed should be within the local calling area and the calls should be of short duration and frequency. Other examples of activities involving the use of government equipment that incur only minimal additional expense include making a few photocopies, using a computer printer to print out a few pages of material, infrequently sending personal E-mail messages or other limited use of the Internet for personal reasons. In addition, short facsimile transmittals within the local calling area are also acceptable.



Use of this equipment should incur only small amounts of electricity, ink, toner, or paper. Long distance telephone calls are only allowed if you call collect, use a calling card, dial an 800 number or third party billing to your home telephone. Unauthorized use of NRC telephones is a violation of MD 2.3 ((D)(3)(b)(c)). The use of the agency's Information Technology for official business has priority over personal use.

During business hours, use of the computer/Internet is perfectly acceptable to access information relevant to official business. Any information that enhances an employee's performance to more satisfactorily perform his or her job is considered acceptable use.

Employees may also use Information Technology to check their Thrift Savings Plan or other personal investments, to seek employment, to communicate with a volunteer charity organization or to file a Freedom of Information/Privacy Act request.

No Expectation of Privacy

NRC employees do not have a right, nor should they expect a right, to privacy when using any agency Information Technology equipment, including the use of E-mail and the Internet. If employees wish that their private activities remain private they should refrain from using NRC Information Technology for personal business. By using government Information Technology, NRC employees consent to disclosing all information contained in the files or passing through any NRC equipment.

Prohibited Use of Government Equipment

Computer Banner

Each time an NRC employee logs onto a government computer, a banner is displayed notifying the user that the computer system is subject to monitoring for maintenance, system integrity, security and for other official purposes. It states in part:

"You should not expect privacy nor protection of privileged communication with your personal attorney regarding information you create, send, receive, use or store on this system. If monitoring reveals possible evidence of criminal statutes, this evidence and any related information including your identification may be provided to law enforcement officials, including the Office of the Inspector General. Anyone who violates the regulations is subject to criminal prosecution and/or disciplinary action."

Statutes & Regulations Restricting IT Use

Management Directive 2.7, Inappropriate Personal Uses (D) further elaborates on the proper and improper use of Information Technology with respect to computers, pagers and telephones. One thing that must be clear about using Information Technology (including the Internet) is that it must **never** be used:

- to view or download any type of pornographic material
- to view or download hate sites about race, religion, disabilities, sexual orientation, national origin
- for illegal gambling and weapons
- to support of "for-profit" activities, i.e., consulting for pay or for sale of goods or services
- in support of a personal/private business
- to gain unauthorized access to other computer systems
- to create, copy, transmit or retransmit chain letters or other unauthorized mass mailings
- to engage in prohibited political activity
- to engage in terrorist activities
- to engage in fund raising activities (except as provided in 5 CFR 950.102)
- to endorse any product or service
- to participate in any lobbying activity or engage in any prohibited political activity
- to post agency information to external newsgroups, bulletin boards or other public forums without authority
- to transmit any type of classified material through the Internet or the NRC servers
- to make personal use of long distance telephone calls or long distance facsimile service, use of message pagers and cellular phones except as permitted by MD 2.3

Con't.

Also Prohibited:

- loading personal software onto government computers
- unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software or data that includes privacy information, copyright, trademark, or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data
- any activity which interferes with official duties.

Office of Government Ethics

The Office of Government Ethics states in Basic Obligation of Public Service, 5 CFR §2635.101 "(b)(5) Employees shall put forth honest effort in the performance of their duties… (9) Employees shall protect and conserve Federal property and shall not use it for other than authorized activities." 5 CFR §2635.704 Use of Government Property (a) *Standard*. An employee has a duty to protect and conserve Government property and shall not use such property or allow its use for other than authorized purpose. (1) *Government Property* includes any form of real or personal property in which the Government has an ownership, leasehold, or other property interest as well as any right or other intangible interest that is purchased with Government funds, including the services of contractor personnel. The term includes office supplies, telephone and other telecommunications equipment and services, the Government mails, automated processing capabilities, printing and reproduction facilities, Government records and Government vehicles.

Yellow Announcement

Yellow Announcement No. 077, "The Use of the Internet at the NRC" dated December 5, 2001, states in part,

"'...NRC employees must exercise common sense, good judgment, and propriety in the use of this valuable resource….

The NRC allows employees to use the Internet for **limited** personal use when such use involves minimal or no additional expense to the government, is performed on the employees' non-work time, does not interfere with the NRC's mission or operation, does not violate the Standards of Ethical Conduct for Employees of the Executive Branch regulations, and is not otherwise prohibited by law.'"

OIG Audit

The Office of the Inspector General performed an audit of Internet usage over an eight day period in June 2001. The results of that audit disclosed that at least 52% and as much as 79% of employee Internet activity was for personal use.

During this audit, a data analysis was performed on computers that had long hours logged into Internet sites. It was determined that in some cases hundreds of hours were logged into pornographic sites. The following examples are brief summaries of OIG cases of inappropriate Internet and government equipment use.

OIG Cases on Misuse of Government Pagers

This OIG investigation determined that over a four month period an NRC manager used an NRC assigned message pager for personal use. The cost to the government was over $1,000.

The employee had previously planned to resign from the NRC. Upon his departure, he reimbursed the government for the expenses incurred.

An NRC contractor employee used his NRC-owned SKYTEL pager assigned to him for personal communications.

Keep NRC issued pagers for business purposes only.

The employee made frequent and lengthy personal pages to another continent which resulted in excess charges to the NRC of almost $1,100. The contractor reimbursed the NRC for the expenses incurred.

The employee was terminated from his position as a result of the misuse of the pager.

OIG Cases on Pornography and Gambling

An Office of the Inspector General investigation revealed that an NRC manager had downloaded pornographic movies and pictures onto his computer.

The manager spent the last 6-12 months viewing and downloading prohibited material from the Internet.

Rather than face administrative action, the manager left the agency.

In several other separate OIG cases, the investigations revealed that several contractor employees downloaded pornographic images and gambling sites onto their computers.

The contractor's employer has agreed to reimburse the NRC for the 89 hours that their employees were engaged in prohibited personal use of NRC computer equipment.

Those contractor employees are no longer employed by the company.

You may use the Internet for personal reasons before and after work or during your lunch break, as long as the use is not specifically prohibited by Management Directive or law.

Con't.

Another OIG investigation determined that an NRC employee had viewed and downloaded pornographic material onto his NRC computer totaling over 75 hours. The employee admitted to OIG investigators that he had been doing this for almost a year. The employee also admitted that he often spent most of his duty hours downloading and viewing pornographic material. He would use as many as 10 diskettes to copy the material depending on the size and quantity of the images he downloaded. Some of the diskettes he used were acquired from the NRC Supply store.

This employee left Federal employment rather than face administrative action.

In another case investigated by OIG, an employee admitted using his computer to view and access pornographic sites.

During the timeframe of May 11 to June 8 he spent almost 7 hours downloading and viewing sites of a sexually explicit nature. The employee admitted to OIG that he knew it was against NRC policy to use an NRC computer for this type of activity.

The NRC employee was suspended for 45 days without pay.

There are other cases currently pending where NRC employees have downloaded images from pornographic sites. The agency has not yet made a determination on these cases.

BEWARE: New ATM Scam—An Actual Case

The last person at the ATM just completed what looked like a simple transaction.

The person is actually rigging the slot on the machine so it will capture the card of the next person.

Rigging is very risky business and requires a "lookout" to warn of possible witnesses and/or potential victims.

The next customer comes to the machine after the trap has been set. He inserts his card and attempts a transaction. The card has been captured and the customer is confused as to why this is so. However, help is on the way...or is it?

Now the perpetrator is pretending to offer assistance. What he really is trying to do is obtain the customer's P.I.N.

He convinces the customer that he will be able to retrieve his card if he entered his P.I.N. while he held down both the "cancel" and "enter" buttons.

After several attempts, the customer is convinced the machine has captured his card. Both the customer and the thief leave the ATM.

Satisfied that the coast is clear, the thief returns to retrieve the card that has been captured by his trap. He not only has the customers card he also has his P.I.N.

Armed with card and P.I.N. he was able to withdraw $1,000 from the account.

United States Nuclear
Regulatory Commission

Mail Stop T 5D-28
USNRC
Washington, DC 20555

Phone: 301-415-5930
Fax: 301-415-5091

Hotline:
800-233-3497

A small section in the U.S. News and World Report, dated January 14, 2002, quoted a memo to State Department Employees: New boss Colin Powell is a nice guy, but he won't excuse those who open porn sites on State Department Internet accounts, join X-rated chat rooms, or send out nasty E-mails. Proof: Probes and punishments are up for those who tap porn sites or send chain letters or jokes of questionable taste.

Office of the Inspector General