August 2005 Volume 3, No. 2

USNRC

OIG Information Digest

NUREG/BR-0304

Use of Information Technology

In June 2001, the Office of the Inspector General (OIG) published an *OIG Fraud Bulletin*[1] that addressed the use of the Government travel card. This bulletin explained the difference between using a personal credit card and a Government-issued travel card. In June 2002, the OIG published an *OIG Fraud Bulletin* that discussed the use of information technology in the workplace, i.e., using fax machines, copying machines, computers, and the Internet for personal as opposed to professional use.

There are still instances where employees use the Government-issued travel card to purchase personal items, or use the computer to download pornography, or to run personal businesses on Government time. Despite Yellow Announcements, warnings, issues of the *OIG Information Digest,* and education about the proper use of Government equipment, the Internet, and Government travel cards, a number of OIG investigations still involve such activity.

This issue of the *OIG Information Digest* will again discuss these topics in an effort to dissuade NRC employees from using their Government-issued travel cards and Government equipment inappropriately. Misusing Government cards and equipment may lead to disciplinary action resulting in lost pay for the employee or even removal from Federal service. Administrative action taken against employees also results in lost time for the Government because those employees cannot be at work to perform their duties. This publication reiterates the importance of using these cards and equipment appropriately. Also included are descriptions of investigations related to these subjects.

Use of Citibank Travel Card

A reminder for all employees is that currently the Government travel card is issued to employees with no application fee, annual fee, interest, or credit check. The card is intended to save the Government the expense of travel advances and to provide employees on official travel a convenient method of handling the expenses associated with that travel. The Government bears the expense of administering the travel card program.

NRC employees are required to adhere to the guidance in NRC Management Directive (MD) 14.1, "Official Temporary Duty Travel," concerning use of the Government-issued travel card. According to MD 14.1, "A card holder may use his or her travel card for official travel," which includes:

- Obtaining authorized travel advances through automated teller machines.
- Paying for official travel expenses such as hotels, meals, and rental cars.
- Obtaining common carrier tick-

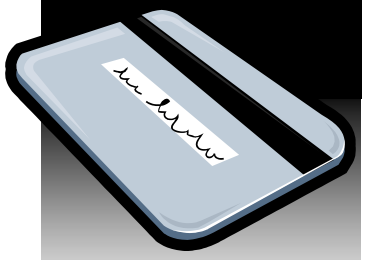
[1]The OIG Information Digest is the successor publication to the OIG Fraud Bulletin.

Special points of interest:

> Use of Information Technology and the Internet

> Stop Unsolicited Mail

> Stop Unwanted Telephone Calls



Inside this issue:

Use of Information Technology (cont. from page 1)

ets when a Travel Management Center (TMC) representative is not available or when the traveler has been specifically authorized to charge his or her ticket.

MD 14.1 states that the travel card may not be used for purchases that would not be reimbursable on the employee's travel voucher and that use of the Government-issued travel card for unauthorized travel advances or personal purchases that are not eligible for reimbursement on a travel voucher may result in disciplinary action.

Travel card statement printouts have been analyzed by the Office of the Chief Financial Officer and the OIG. Some of these statements indicated that items and services such as those listed below have been improperly purchased with the Government travel card:

- Engine repairs, gas, oil change, battery for personal vehicles
- Clothing
- Doctor visits
- Medical outpatient procedures
- Personal travel
- Personal entertainment
- Meals when not in travel status
- Casino transactions
- Groceries
- Hotels for personal travel
- Cash withdrawals for personal use
- Cable television service

Yellow Announcements

Between 1999 and 2000, NRC issued three Yellow Announcements regarding the use of Government travel cards. Beginning in March 2000, the Office of the General Counsel incorporated into its annual ethics briefing, guidelines on the appropriate use of the Government travel card. Since that time, NRC has also provided annual notices to all NRC employees on the subject.

Cases on Misuse of Government Travel Card

1. During an 18-month period, an NRC employee used the Government travel card to withdraw almost $6,000 in cash for personal reasons. This employee also withdrew more than $9,000 greater than the authorized amount allowed for official travel in the same time period. The employee is facing removal from Federal service.

2. An NRC consultant made 58 personal purchases totaling more than $10,000 on the Government travel card. These purchases were not made in connection with any official NRC business and, according to NRC travel records, the consultant had not traveled on official NRC business since 1998. The consultant's appointment with NRC was terminated.

3. An NRC employee used the Government travel card to make more than $2,500 in personal purchases for gasoline, medical treatment, entertainment, and other miscellaneous expenses. These purchases were not made in connection with official travel. The employee was suspended for 5 days.

4. Another NRC employee used the Government travel card for excessive cash advances which were claimed for official business. This employee was late paying the travel card bill and also made false statements to OIG concerning payment schedule and checks returned for insufficient funds. The travel card account was canceled and the employee was suspended for 30 days.

5. An NRC employee made 60 personal purchases for more than $6,000 using the Government-issued travel card. The purchases were for retail and online purchases, Internet and satellite TV service, and other miscellaneous items. The employee was suspended for 5 days.

Proper Use of Information Technology and the Internet

As beneficial as the appropriate use of the Internet can be, the repercussions for misuse by a Government employee in the workplace can be costly. Federal employees are prohibited from accessing certain Web sites using Government computers. Employee productivity may also be affected by excess personal use of the Internet. Additionally, NRC contractors may not use the Internet for any type of personal use.

Use of the Internet is a privilege, not a right. Misuse of Government information technology resources is considered misconduct and employees involved in such activity could be subject to disciplinary action. Accessing pornographic sites is an example of this type of misconduct.

Statutes, regulations, and NRC Management Directives all provide guidance on the proper and improper use of Government equipment.

NRC MD 2.7, "Personal Use of Information Technology," provides that NRC extends the opportunity to its employees to use Government property for personal purposes in an effort to create a more supportive work environment. MD 2.7 states that the policy grants a privilege--not a right--to use agency information technology for certain non-Government purposes.

Use of NRC information technology for personal purposes is acceptable provided such use involves 1) minimal or no additional expense to the Government, 2) is performed before or after work or during a lunch period, 3) does not interfere with NRC's mission or operations, 4) does not violate the Standards of Ethical Conduct for Employees of the Executive Branch, and 5) is not prohibited by law. These guidelines apply to use of personal computers, printers, software, telephones, pagers, facsimile machines, photocopiers, e-mail, and the Internet. However, MD 2.7 prohibits an employee from using the Internet to access sites on pornography, hate crimes and gambling.

During business hours, use of the computer/Internet is acceptable to access information relevant to official business. Any information that enhances an employee's ability to better 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, seek employment, communicate with a volunteer charity organization, or file a Freedom of Information/Privacy Act request.

No Expectation of Privacy

NRC employees do not have a right to, nor should they have an expectation of, privacy when using any agency information technology equipment, including e-mail and the Internet. If employees wish their private activities to remain private, they should refrain from using NRC information technology for non-Government purposes. By using Government information technology, NRC employees consent to the disclosure of all information contained in the files or passing through NRC equipment.

<u>Computer Banner</u>

Each time an NRC employee logs onto an NRC Government computer, a banner is displayed notifying the user that the computer system is subject to monitoring for maintenance, to preserve system integrity and 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 violation 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 security regulations or makes use of Federal computer systems is subject to criminal prosecution and/or disciplinary action.

Proper Use of Information Technology and the Internet (cont. from page 3)

Statutes and Regulations Restricting IT Use

Management Directive 2.7 provides examples of the improper use of information technology with respect to computers, pagers, and telephones. All employees should be familiar with its content. All employees are expected to be responsible for their own personal and professional conduct.

OIG Cases on Misuse of Computers

Three contractor employees received and forwarded e-mails to each other that contained sexually explicit images. They used their assigned NRC e-mail accounts to forward these to each other for a period of about 15 months. These contractors were terminated from their positions.

An NRC resident inspector knowingly misused his NRC-assigned computer to access sexually explicit Web sites. He claimed he normally spent about 1 hour, two to three times a week viewing Internet Web sites containing sexually explicit material. He had approximately 9,000 files containing nude images on his computer, including nude images of individuals who looked to be under age 18. The employee elected to retire from Federal service rather than face administrative action. (Legal action was not warranted because none of the images met the legal standards for child pornography.)

An NRC employee knowingly misused his NRC-assigned computer to access Web sites of a sexual nature and sent sexually explicit messages to coworkers over the Internet two or three times a day. The employee claimed he viewed these sites for approximately 20 to 30 minutes every day. He also created files of images of nude or partially nude individuals and stored the images on the NRC computer network storage area assigned to him. The employee was suspended for 45 days without pay.

Eleven NRC contractor employees engaged in prohibited Internet activity by viewing sites of a pornographic nature. The employees also searched the Internet for personal reasons. The total hours spent on computers for non-business related work exceeded 725. NRC was able to recover more than $61,000 from this contractor company. Internet access has been removed from the computers of these contractor employees.

An NRC employee reported that he thought someone was trying to access his NRC computer and he asked for help resolving this problem. During a review of his computer, many files containing sexually explicit materials were discovered. OIG also discovered that the employee had been creating sexually explicit stories to post on the Internet. This employee was issued a 20-day suspension without pay.

An NRC employee decided to retire rather than face administrative action because on more than one occasion he left on a printer sexually explicit material which he had downloaded from the Internet.

An NRC employee admitted using his NRC-assigned computer to download and view sexually explicit material ever since the NRC provided Internet access through its network. He claimed he spent many hours viewing pornography. This employee was issued a 21-day suspension without pay.

An NRC employee sent harassing and threatening e-mails from an NRC computer and also used a telephone to make harassing calls. The employee was arrested and sentenced to 1 year of probation and community service for using a personal telephone to place harassing calls. NRC issued the employee a Letter of Reprimand for inappropriately using the agency e-mail system.

OIG Cases on Misuse of Computers (cont. from page 4)

An NRC employee frequently used the NRC computer, e-mail system, and telephone to conduct outside personal business. Action is still pending on this investigation.

This is only a sample of cases that OIG has investigated concerning the misuse of information technology.

Stop Unsolicited Mail!

OIG is reprinting information from the last *OIG Information Digest* on how to stop unsolicited mail and phone calls. Too frequently, our mailboxes are cluttered with unsolicited offers of credit cards preapproved for amounts ranging from $5,000 to $25,000 with low interest rates. We are also consumed with advertisements for life insurance policies. Would you like to stop being barraged with all this "junk" mail? The credit bureaus are offering a toll-free number that lets you "opt-out" of all these offers. Call 1-888-567-8688 for an automated message. You will be prompted for personal information. Alternatively, you may "opt-out" by accessing the Web site at www.optoutprescreen.com. You will be required to provide personal information. This is a secure site and also has an additional mechanism in place to ensure security and privacy. OIG spoke with two Experian employees concerning requirements to opt-out and was assured that the two methods were very secure.

Stop solicitations from the Direct Marketing Association's 5,200 member companies, which represent 80 percent of these marketers. Get forms for $5 at www.dmaconsumers.org/cgi/offmailinglist. Or write for free forms to the Direct Marketing Association, Mail Preference Service, P.O. Box 643, Carmel, NY 01512.

Remove yourself from some mortgage refinancing and home equity loan offers by calling the Axciom U.S. Consumer Hotline at (877) 774-2094 or writing to DataQuick, Attn: Opt-out Department, 9620 Towne Center Drive, San Diego, CA 92121.

Stop Those Phone Calls!

You may reduce the number of telemarketing calls on your home phone and cell phone by dialing 1-888-382-1222. Your request will stay in the registry for 5 years unless the phone is disconnected or you remove your number from the registry.

If you have any questions or concerns relating to the use of the Government travel card or use of NRC information technology equipment, please consult MD 2.7 or call the Office of the Inspector General.

You may report fraud, waste, or abuse, by writing to:

NRC
Hotline Program
Office of the Inspector General
Mail Stop T5D28
11545 Rockville Pike
Rockville, MD 20852

Or you can call:

800-233-3497
TDD
800-270-2787

Or you may also:

Access the NRC Web site, click on Inspector General, click on Hotline, type your complaint, and click submit.