U.S. NUCLEAR REGULATORY COMMISSION

NUREG/BR-0304—August 2003

Volume 1, Number 1

OIG Information Digest

Special points of interest:

- Audit News
- Investigative News
- Do's and Don'ts Concerning Internet Use

Introduction

The Inspector General's Office has renamed this publication from *OIG Fraud Bulletin* to *OIG Information Digest.* This change reflects that we have broadened the scope of the publication to include topics beyond the subject of fraud.

In this and future issues, topics may include:

- The operation and purpose of this office,
- Audits and investigations of interest,
- Do's and don'ts in the workplace,
- Scams that can affect your personal life,
- More information on identity theft,
- How to protect yourself and your home,
- Trends of our current and past investigations, and
- Summaries of some of the more prevalent cases of wrongdoing that occur within NRC and other agencies.

We hope this information will prove valuable to you in your professional and personal life.

Use of the Internet

The use of the Internet in the workplace and associated privacy concerns represent one of the more troubling issues of our time. While the Internet is fast and inexpensive, Internet usage can pose significant risks if it is not managed or is abused. The various forms of Internet activity have become ingrained in most corporate cultures. Today, roughly 90 million business workers in the United States (about two-thirds of all workers) and about 120 million workers outside the U.S. use the Internet. E-mail has replaced the telephone as the primary and preferred method of business communication for those with Internet access.[1]

The Internet provides computer access to an ever-expanding storehouse of electronic information through the mass connection of networked computers. Use of the Internet offers tremendous capabilities to employees in terms of access to a wide variety of information sources relevant to their official duties. However, 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 work place. Abuse, misuse,

Internet Use

(cont. from page 1)

and overuse by employees can in egregious cases:

- Leave employers vulnerable to lawsuits (downloading of sexually explicit material has been viewed as creating a hostile work environment);
- Introduce various security issues, such as the release of confidential, proprietary, or otherwise sensitive information, or a download of unlicensed software or viruses;
- Cause a decline in employee productivity; and
- Strain network resources.

Implementing a comprehensive Internet usage policy clarifies usage guidelines and directives designed to inform and educate employees about proper practices with regard to Internet activity.

Organizations also adopt technical measures, including:

1) Tools to monitor Internet activity to enforce policy and identify offenders,

2) Antivirus utilities to protect against malicious code at all potential points of infection,

3) Secure e-mail solutions to protect information traveling across the Internet, and

4) Archiving utilities and storage systems to ensure that messages are deleted or retained as appropriate.[2]

A recent American Management Association survey[3] found that more than three-quarters of major U.S. firms (almost 78 percent) record and review employee communications and activities on the job, including Internet use. This figure has doubled since 1997. Based on recent Government audit reports, there is compelling evidence of the same need for surveillance in the Federal Government.

A Privacy Foundation study found that many employers regularly monitor employee e-mail and Web surfing.[4] Monitoring refers to the management policies, processes, and supporting technology for ensuring compliance with organizational and agency privacy guidelines and the ability to exhibit due diligence. Monitoring also refers to the conduct of internal and external independent reviews and audits to ensure compliance with legislation and regulations.[5] The study estimated that 14 million employees were under continuous Internet or e-mail monitoring using commercially available software.

Currently, practice is that Federal employees are permitted limited personal use of the Internet if the use does not interfere with official business and involves minimal or no additional expense to the Government. This limited personal use is to be performed on the employee's non-work time. The policy also outlines the following inappropriate personal uses of Government office equipment:

- Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment;
- Downloading of malicious files and vulnerable software, and the download and use of unlicensed software;
- The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials,
- The creation, downloading,

When users log into NRC's LAN they see the following language:

!USE OF THIS COMPUTER CONSTITUTES A CONSENT TO MONITORING.

Anyone who violates security regulations or makes unauthorized use of Federal computer systems is subject to criminal prosecution and/or disciplinary action.

Internet Use (cont. from page 2)

viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, or any other illegal activities otherwise prohibited.[6]

Private industry also uses models for Internet usage. The ePolicy Institute has developed a sample employee Internet usage policy. Covered employees sign a statement that acknowledges that they have read and agree to abide by the Internet policy as consideration for continued employment.

The ePolicy Institute also developed Do's and Don'ts to help employers decide what is an acceptable risk for the organization.

The Do list includes:

- Establish comprehensive, written ePolicies that address employee use of e-mail, the Internet, and software;
- Communicate that the organization's Internet systems are to be used strictly as business communication tools;
- Review the written ePolicies with every employee;
- Incorporate the policy into employee handbooks;
- Address ownership issues and privacy expectations; and
- Require that each employee reads, signs, and dates a hard copy of the policy.

The Don't list includes:

- Don't rely solely on e-mail to communicate the ePolicies;
- Don't expect employees to train themselves on the policies.[7]

NRC Management Directive 2.7 contains the NRC's guidelines for employees' personal use of information technology.

The Directive outlines the conditions under which employees may and may not use the agency's information technology capabilities.

Sources of Information

1. E-mail and Internet usage policy statistics developed by industry analyst Jonathan Penn for the infoshop.com. (September 17, 2001).
2. Internet information provided by Jonathan Penn, industry analyst for the-infoshop.com Web site (September 17, 2001).
3. American Management Association's 2002 Survey on Workplace Monitoring and Surveillance (August 2001).
4. Workplace Surveillance Project of the Privacy Foundation, a research group based at the University of Denver, conducted this study in July 2001.
5. This definition is offered by Robert Parker in an article for the Information Systems Control Journal (September 2001).
6. "Limited Personal Use" of Government office equipment recommended by the Federal CIO Council in May 1999.
7. These examples come from the ePolicy Handbook published by the ePolicy Institute in 2001.

NRC Employees and Contractors Using Computers to Download Pornography

In June 2002, OIG published a Fraud Bulletin dedicated to the use of information technology in the workplace. In that issue, descriptions were provided regarding the proper and improper use of telephones, pagers, fax machines, photocopiers, e-mail, computers, and the Internet.

Of particular note was the concern that NRC employees were using the Internet to view sites of a pornographic nature. Management Directive 2.7 strictly prohibits the use of NRC computers to view or download this type of material.

OIG performed an audit in June 2001 of Internet usage over an 8-day period during that month. It was determined that in some cases hundreds of hours were logged into pornographic sites.

NRC employees and contractors continue to use NRC computers to view and download material from pornographic sites. Subsequent to the publication of that audit report, 30 cases have been investigated resulting in 8 suspensions for a total of 251 calendar days of lost time and lost salaries of approximately $62,124. In addition, seven individuals either resigned or were terminated rather than face administrative action. Three cases resulted in reimbursement for time used on the computer by contractors, four cases are currently pending NRC management action, and seven cases are still under investigation by OIG.

The time each individual was suspended without pay varied from 10 to 45 days.

The audit component of OIG has another initiative underway to determine the extent of Internet use by NRC employees.

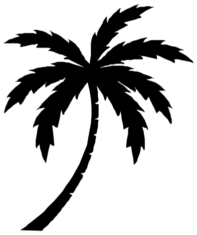
NRC contractors may not use Government computers for any personal reasons, including to access the Internet or to communicate via e-mail.

It is important to remember that NRC computers are NEVER to be used for illicit or illegal purposes. To do so can place an employee in the position of facing significant disciplinary action.

Beware of Travel Fraud (Article from the National Consumers League)

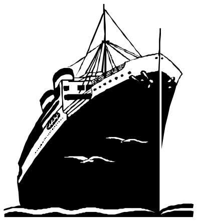
The prospect of getting away to a warm romantic island or visiting a foreign country is extremely appealing. But what may seem to be a bargain may in fact be a nightmare.

Be skeptical of offers for "free" trips. Airlines and other well-known companies sometimes operate contests for travel prizes. However, there are also companies that offer "free" trips to try to lure people into buying their products or services. It's never "free" if you have to pay something.



Know exactly what's included. A "free" or incredibly cheap trip may have hidden costs. For example, the cruise may be free, but you have to pay to fly to the departure point and stay in a hotel at your own expense. Or you may have to endure a long, high-pressure sales pitch for a timeshare or travel club membership as part of the trip.

Realize that the deal may not be as good as you think. You may find that a travel offer requires you to make reservations through a specific company and that the costs are higher than they would be if you used your own travel agent or made the arrangements yourself. Alternatively, the offer may be valid only if you bring a companion along at full fare.



Be aware of restrictions. Often the best travel deals are available only for off peak times, not during school vacations, holidays, or other popular travel dates. You may find it hard to get the promised price for the dates that you want to

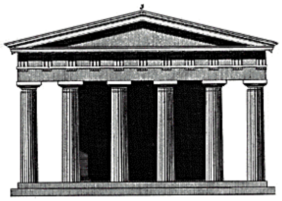
Travel Fraud (cont. from page 4)

travel or there may be no space available on those dates at all.

Confirm the arrangements. If transportation and hotel are included in the travel package, ask how to contact those companies and confirm with them directly that the reservations have been made.

Do your own travel research. It's easy to get information from a local travel agent and other sources such as newspapers, books, and the Internet. You may be able to get the trip you want for far less than the "bargain" price a company is offering.

Pay with a credit card. Fraudulent travel operators take the money and run and even legitimate companies can suddenly go out of business. Protect yourself by paying with a credit card so you can dispute the charges if the promises aren't kept.

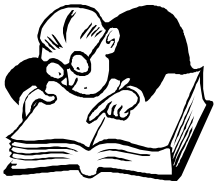


OIG Audit Program

Recently Completed Audits

Audit of NRC's Regulatory Oversight of Special Nuclear Materials (OIG-03-A-15), May 23, 2003

OIG found that NRC's current levels of oversight of licensees' material control and accounting (MC&A) activities do not provide adequate assurance that all licensees properly control and account for special nuclear material. Specifically, NRC performs limited inspections of licensees' MC&A activities and cannot assure the reliability of the Nuclear Materials Management and Safeguards System data.



NRC's Oversight of Research and Test Reactors (OIG-03-A-16), June 5, 2003

The OIG determined that NRC's oversight of research and test reactors was meeting NRC's expectations, however, some aspects of oversight can be improved, including (1) guidance for inspection followup items, (2) operating plans, (3) information available to the public, and (4) documentation for refresher and continuing inspector training.

Memorandum Report: Review of NRC:s Purchase Order Processing (OIG-03-A-17)

The Division of Contracts and the Division of Financial Services have non-integrated computer systems and agency program offices have their own office-specific invoice tracking systems, all of which require entry of the same or similar information. Both organizations are currently working together to develop an E-Procurement system. Close intra-agency coordination is needed to ensure that this initiative, as well as process improvements in the commercial payments area, are successful.

Audits in Progress

Internet Follow Up - The objective of this audit is to determine how newly implemented controls affect use of the Internet.

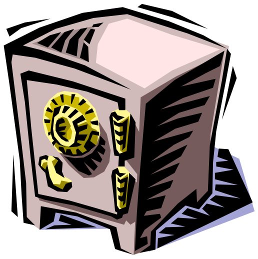
Review of NRC's Personnel Security Program - The objective of this audit is to evaluate NRC's access and clearance process for employees and contractors and whether the program is effectively managed.

Audit of NRC's Contract Administration Practices - The objective of the audit is to review the economy, efficiency, and effectiveness of the management controls included in the NRC's contract administration program.

Audit of NRC's FY 2003 Financial Statements - The objective of the audit is, in part, to evaluate internal controls, and review compliance with applicable laws and regulations.

The Audit Program

Audit of NRC's Protection of Safeguards Information **-** The objective of this audit is to determine whether NRC adequately defines what constitutes safeguards information, ensures its protection, and prevents inappropriate release to unauthorized individuals.



Independent Auditor's Report

Closeout Audit of GSE Power Systems, Inc. (OIG-03-A-19)

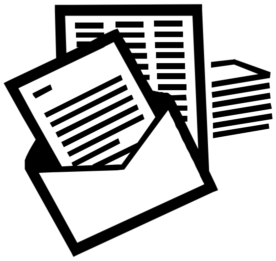
This report reflects the results of a review to determine the allowability and allocability of the direct and indirect costs claimed in the closeout documents. The audit disclosed that GSE did not maintain sufficient reports to support contract costs, which is failure to comply with the requirements of the Federal Acquisition Regulations (FAR) 52.215-2, *Audit Records—Negotiation,* which is incorporated in the contract by reference. The audit also recommended disallowance of some contract costs.

OIG Investigative Program

Inappropriate Handling of an Enforcement Action by Region III

OIG conducted an investigation into several concerns about the handling of an enforcement action related to prohibited employment discrimination by Exelon Nuclear Generation Company, an NRC licensee. It was alleged that (1) NRC erred in settling the enforcement action in that the action violated NRC's enforcement policy and (2) NRC ignored findings that an Exelon manager deliberately discriminated against an employee for engaging in a protected activity. In addition, it was alleged that NRC conducted closed meetings with Exelon to discuss a settlement of NRC's enforcement action without the knowledge of the employee's attorney and contrary to promises made by NRC.

As a result of the investigation, OIG determined that because the licensee admitted violating NRC regulations pertaining to prohibited employment discrimination, NRC exercised enforcement discretion and settled the matter prior to holding an enforcement conference. OIG learned that while settlement of an enforcement action prior to holding an enforcement conference is unusual, this action was coordinated with NRC's Office of the General Counsel and the Office of the Executive Director for Operations. Additionally, OIG found that the settlement did not violate NRC's Enforcement Policy, as the Enforcement Policy is silent regarding the timing of negotiated settlements. OIG also found that the Exelon employee's attorney was not excluded by NRC staff from participating in NRC enforcement proceedings because no formal enforcement meetings took place. In addition, OIG found that on October 3, 2002, NRC issued a Confirmatory Order to Exelon which confirmed the licensee's commitment to train its managers at all Exelon plants concerning NRC requirements related to maintaining a safe work environment.



OIG Investigative Program

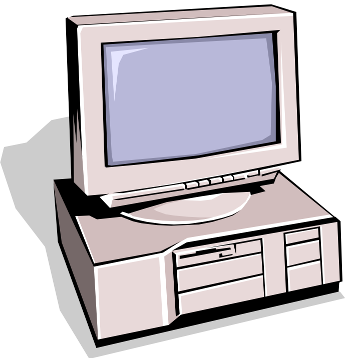
(cont. from page 6)

Fraud by NVT Involving NRC Custodial Contract

OIG conducted an investigation into information provided by a former Nguyen Van Thanh Technologies (NVT) employee alleging that NVT failed to meet several contract requirements involving preventive maintenance. NVT had a 5-year building maintenance contract with NRC in the amount of $5 million.

As a result of the investigation, OIG found that the NVT project manager for the NRC contract instructed the former NVT employee to falsify entries in generator and fire pump log books for the emergency lighting and fire sprinkler systems at NRC headquarters buildings between February 2000 and January 2001. These entries made it appear that this safety equipment was tested, as required by the NRC contract, when in fact such testing had not occurred.

In March 2002, the project manager for NVT and the corporation were indicted by a Federal Grand Jury in the Southern District of Maryland on 12 counts of violation of Title 18 United States Code (USC), Section 1001, False Statements, and 18 USC, Section 2, Aiding and Abetting. The indictments against the NVT project manager and NVT were subsequently dismissed in lieu of a civil settlement by the U.S. Attorney's office.



We're on the WEB!
Access the HOTLINE
Thru the NRC Website!

Organization

U.S. Nuclear Regulatory Commission
Office of the Inspector General
11545 Rockville Pike
Rockville, MD 20851

Hotline Number—800-233-3497
Fax - 301-415-5091