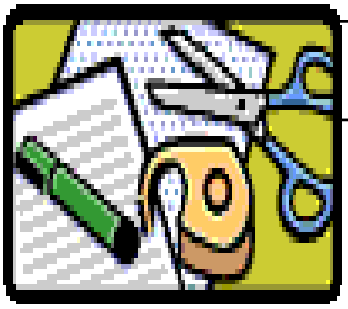
OIG Information Digest

NUREG/BR-0304 Volume 4 ,Number 2 October 2007



Property and Supplies

Inside this issue:

The Federal Government spends billions of dollars each year to purchase equipment and supplies. Unfortunately, a significant percentage of these items are stolen or misused, wasting our tax dollars and impeding the agencies' ability to perform their missions. In this issue of the OIG Information Digest, we are going to cover some of the responsibilities each employee has to exercise good stewardship over government equipment. We've included several examples of property theft and diversion from across the government. Hopefully, this information will help all of us keep the NRC's resources focused on supporting our responsibilities to regulate the nuclear industry.

Individual Responsibilities

Regulations should be adhered to when using Government equipment and supplies. Management Directive 13.1 outlines the use of property and supplies by NRC employees to provide sufficient controls to deter or eliminate loss through fraud, waste, or misuse.

As outlined in Management Directive 13.1, Part I, NRC employees have the responsibility to:

- Properly care for, protect, and conserve NRC property assigned to them.
- Use NRC property for officially approved purposes only, including property leased to the NRC.
- Promptly report the loss, damage theft, destruction, or removal of property from its assigned location.
- Account for all property listed on receiving documents (i.e., parking slips, receipts, invoices) before acceptance and provide copies of the documents to the property custodian.
- Sign NRC Form 119 before receiving custody of sensitive property.

Supplies

Supplies are readily available to all headquarters employees in the self-service Supply Store located on the P1 level of One White Flint North. NRC contractor personnel may not directly request Government-furnished supplies nor use the Supply Store. If authorized by the contract, project officers may request supplies for contractor use or accompany contractors to the Supply Store.

Unneeded supplies should be returned to the Supply Store or placed in supply return boxes located in each building. Specific locations for these boxes are given on the ADM Web site, Administrative Services Home Page, under "Recycling." Returned supplies will be examined by store personnel to determine if they are reusable.

Property and Supplies (con't from page 1)

Usable supplies will be placed on Supply Store shelves, and NRC employees are encouraged to reuse these items rather than take new supplies. These supplies are not to be used for personal use nor to take home and use as school supplies for children or for a personal business or other personal activities.

Theft of Government Property

Theft of Government Property at Headquarters should be reported as soon as possible to the nearest guard station. The guard will complete a Security Incident Report and submit it to the Chief of the Physical Security Branch (PSB). He will then forward the results of his investigation along with a copy of the NRC Form 1345 to OIG within 24 hours after the loss or suspected theft. If the theft occurs at a regional office or a remote NRC location, the employee must notify the Property Custodian, Physical Security Branch, and the IG within 24 hours of the loss or suspected theft.

If a theft occurs outside of NRC space the employee should immediately notify the proper law enforcement authority. It is the responsibility of the employee to file claims with airlines or insurance carriers for all government property as soon as possible after theft occurs. Employees must remember to provide a copy of the police report and statements received from the insurance company as supporting documentation for NRC records. If the property is not found within 10 days, the employee's Property Custodian will fill out form 395 and submit to the Chief of PSB.

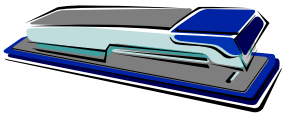
Financial Liability

Employees may be held financially liable for any missing or damaged government property assigned to them. If found liable the employee will be required to pay the government the depreciated value for the lost or stolen equipment if found to be the fault of the employee due to careless disregard or a "willful act." Employees should provide the degree of care for Government property as they would their personal property.

Property Custodians Responsibilities

There is much more emphasis placed on Property custodian duties and responsibilities than individual employees. Property custodians are responsible for

maintaining an effective, efficient, and accurate property management program.



According to Management Directive 13.1 Part I, Property Custodians must:

* Ensure that property holders are made aware of their responsibilities for the use and care of NRC property at the time the property is assigned to them.
* Participate in official property inventories by accompanying the DCPM inventory team, assisting in locating missing equipment, and providing purchase documentation for any non-tagged equipment.
* Attend periodic training provided by ADM to keep current on procedures governing the agency's property management program.
* Tag new equipment immediately upon receipt and forward the tag assignment sheet and purchase documentation to DCPM no later than 5 days after the tag is placed on equipment.
* Keep tags secure at all times and use tags sequentially. Ensure that there are no gaps in tag numbers assigned. (The SPMS system administrator must assume that gaps serve as an indication that property has been tagged but acquisition documentation has not been provided to DCPM in a timely manner.)

NOTE: For complete information consult MD 13.1.

Audit of NRC'S Non-Capitalized Property

A recent OIG audit was conducted to determine whether NRC has established and implemented an effective system of management controls for maintaining accountability and control of non-capitalized property.

While NRC's property management policies for non-capitalized property provide a framework to control and safeguard property, the program, as implemented, needs improvement to provide effective control. Specifically:

* SPMS data is not accurate;
* Controls for Information Technology (IT) property that may contain personally identifiable information (PII) are lacking;
* Physical security deficiencies exist; and
* The policy for notifying Office of the Inspector General (OIG) of missing property needs improvement.

In light of NRC's imminent growth in full-time equivalents (FTE), and anticipated office relocations, it is increasingly important that NRC maintain effective and efficient accounting and control over non-capitalized property. Therefore, now is an opportune time for NRC management to increase accountability for, and improve control of, the property management program. An effective and efficient property management program is essential to assure that staff have the property needed to carry out their duties and assure optimum utilization of staff time, property and fiscal resources.

Recommendations from Audit Report

This report made recommendations to the Executive Director for Operations to help NRC strengthen the effectiveness of management controls with respect to maintaining accountability and control of non-capitalized property. This report also recommends that the threshold for accountable non-sensitive property be raised so that property custodians can focus on maintaining accurate and reliable property records for sensitive and more expensive items.

Note: The full audit report may be found on NRC's public web site.

Property Audit of the FBI by GAO *(http://www.gao.gov/new.items/d06306.pdf)*

Major Lapses in Accountability Resulted in Millions of Dollars of Missing Trilogy Equipment

The FBI did not adequately maintain accountability for computer equipment purchased for the Trilogy project. The FBI relied extensively on contractors to account for Trilogy assets while they were being purchased, warehoused, and installed. However, the FBI did not establish controls to verify the accuracy and completeness of contractor records it was relying on, to ensure that only the items approved for purchase were acquired by the contractors, and to ensure that it received all those items acquired through its contractors. Once the FBI took possession of the Trilogy equipment, it did not establish adequate physical control over the assets. Consequently, it was found that the FBI could not locate over 1,200 assets purchased with Trilogy funds, which were valued at approximately $7.6 million. In addition, during its physical inventory counts for fiscal years 2003 through 2005, the FBI identified over 30 pieces of Trilogy equipment valued at about $167,000 that it reported as having been lost or stolen. Due to the significant weaknesses identified in FBI's property controls, the actual amount of lost or stolen equipment could be even higher.

Conclusions

FBI's Trilogy IT project spanned 4 years and the reported costs exceeded $500 million. The review disclosed that there were serious internal control weaknesses over the process used by FBI and GSA to approve contractor charges related to Trilogy, which made up the vast majority of the total reported project cost. While this review focused specifically on the Trilogy program, the significance of the issues identified during the review may be indicative of more systemic contract and financial management problems at FBI and GSA.

Stolen DOT Computers (http:www.fcw.com/article96913-11-22-06-Web))

An investigation into two recent laptop computer thefts from the Department of Transportation's (DOT) Office of Inspector General (OIG) has helped uncover a ring of laptop thieves, according to the latest status report on the incidents.

On July 27, someone stole a DOT OIG special agent's laptop from a locked car near Miami. The laptop contained personally identifiable information on about 133,000 Florida residents. Following that episode, officials reviewed an April theft of an OIG laptop that occurred in Orlando, FL.

It took several weeks for computer crime forensics experts to check the Orlando laptop's backup files for sensitive personally identifiable information (SPII), an OIG spokesman said.

"They found about 9,000 individuals [who] were also on the Miami-area laptop and about 900 who were not on the Miami-area laptop," he said.

Nearly all the individuals had been entered into the Orlando computer as part of a criminal investigation into fraudulent licensing. The individuals were not suspects. Rather, they had picked up their commercial driver's licenses, airman certificates, and security clearances from facilities where incidents of fraud had been reported. The laptop also contained a small number of employee records, such as leave approvals and employee evaluations.

Although both laptops were protected with passwords, the contents — including names, Social Security numbers and addresses — may or may not have been encrypted. The data on the Miami laptop was definitely not encrypted, according to OIG officials, but it is unclear whether the contents of the Orlando laptop were encrypted. "This still has not been determined with absolute certainty. It was to the best of our knowledge not encrypted when the laptop was stolen." "The SPII data had been encrypted previously, but the encryption software had been disabled to allow migration of a server and updating of software."

He added that OIG officials do not know for sure whether it was unencrypted at the time of the theft because the scripts controlling the encryption process were not visible to the computer's owner.

Officials are confident that the laptops were not targeted for identity theft. No credit fraud has resulted from the theft of either computer, the report states.

"Based on the investigation to date, we believe that the risk of credit fraud in the future is very low. The investigation is nearly complete and we expect to issue a report by the end of the year," according to the status report.

The laptop investigation — which was undertaken by OIG special agents, with assistance from the FBI and Miami-Dade County Police Department — led to the arrest of an individual suspected of stealing the Miami-area laptop, according to the report. During surveillance at the same restaurant where the laptop had been stolen, the suspect stole a decoy computer — using the same technique that was used in the original theft. He used a device to punch the lock in the passenger-side door.

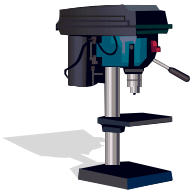
The suspect acknowledged stealing many laptops but did not acknowledge taking the laptop on July 27. This individual was indicted on a federal charge of theft of government property for stealing the decoy laptop.

Interviews with the individual and others involved uncovered a small theft ring in which its members stole laptops at the restaurant and in the nearby vicinity. The ring members would load the stolen laptops with new operating systems and then sell them on the used computer market, primarily to high school students, the OIG status report states.

DOT OIG and an identity risk management contractor found no indications that any of the affected individuals' personally identifiable information had been misused.

A hotline established to address citizens' concerns has received more than 1,600 phone calls, e-mail messages and letters. Nearly 50 of those communications produced possible leads in the criminal investigation.

Press Releases on Stolen Property *(http://www.dodig.osd.mil/hotline/.)*



Navy Seabees Implicated in the Sale of Government Owned Tools -The Office of the Inspector General Department of Defense announced that based on allegation received by the Defense Hotline, an investigation determined that Navy Seabees sold Government-owned tools and parts on eBay.

The anonymous source identified a petty officer second class as being involved. During the course of the investigation federal search warrants were executed at residences in Riverside County and San Diego County, CA. Several sailors were identified as co-subjects and interviewed, resulting in five confessions and the recovery of MAC Tools valued at $5,000.00.

Further investigation disclosed three additional sailors involved in the forgery of open purchase requests and purchasing items for personal gain. The estimated loss to the Government totaled $18,602 in HMMVV parts, MAC tools and Snap-on tools.

A total of seven Navy petty officers were either court-martialed or accepted non-judicial punishment. Punishments included imprisonment, fines, reduction in grades and several bad conduct discharges.

Office of the United States Attorney (**Eastern District of Kentucky)**

http://www.dodig.osd.mil/IGInformation/IGInformationReleases/July2006GJpressreleases.pdf

A United States Attorney for the Eastern District of Kentucky, and Resident Agent In Charge, Department of Defense, Defense Criminal Investigative Service, jointly announce that a federal grand jury in Lexington returned an indictment charging an unnamed person with a violation of Federal law. The indictment alleged from 2003 until April 2006, an employee of the Special Operations Forces Support Activity (SSA) in Lexington, KY, stole military equipment from SOFSA. He reportedly sold the items on eBay. If convicted, the maximum potential penalties are 10 years imprisonment, a fine of $250,000 and supervised release for a period of 3 years.

U.S. Department of State Case *(http://oig.state.gov/oig/inv/summaries/14422.htm)*

The Department of State (DOS) OIG received information that a private citizen was selling computers and office equipment bearing U.S. DOS property tags on the Internet and at yard sales he was holding at his residence. A joint investigation conducted with the Coral Springs, Florida, Police Department determined that the private citizen had obtained the property from the Department's Regional Procurement Support Office, Florida Regional Center, under false pretenses. The property in question had been classified as excess, and was supposed to have been donated to a charitable organization. The investigation determined that the subject of the investigation misrepresented himself as belonging to the charitable organization that was supposed to receive the property.

A search warrant of the subject's residence resulted in the recovery of $30,543 in stolen U.S Government property. Furthermore, records obtained from the Internet company showed that the subject had earned an additional $5,562 in proceeds from illegal sales of U.S. Government property. The subject was subsequently arrested and pled guilty to a 3rd Degree Grand Theft Felony Charge under State of Florida code. He was sentenced to two years probation and ordered to pay $373 in court costs.

This issue of the OIG Information Digest contained information on the responsibilities of government employees for property and supplies. In addition, we would like to provide some facts on the latest scams affecting all individuals.

Something Vishy *(http://www.fbi.gov/page2/feb07/vishing022307.htm)*

It's one of the latest breakthroughs in telecommunications—**Voice Over Internet Protocol, or VoIP**, which enables telephone calls over the web...**and guess who's hopping on the VOIP bandwagon along with millions of legitimate customers?** Criminals, that's who. They're using the technology to hijack identities and steal money. It already has a name: "vishing."

New wine, old wineskins. Vishing is really just a new take on an old scam —phishing. You know the drill: you get an e-mail that claims to be from your bank or credit card company asking you to update your account information and passwords (perhaps, it says cleverly, because of fraudulent activity) by clicking on a link to what appears to be a legit website. Don't do it, of course. It's just a ruse, nothing more than an illegal identify theft collection system.

Vishing schemes are slightly different, with a couple of variations.

* In one version, you get the typical e-mail, like a traditional phishing scam. But instead of being directed to an Internet site, you're asked to provide the information over the phone and given a number to call. Those who call the "customer service" number (a VoIP account, not a real financial institution) are led through a series of voice-prompted menus that ask for account numbers, passwords, and other critical information.

* In another version you're contacted over the phone instead of by e-mail. The call could either be a "live" person or a recorded message directing you to take action to protect your account. Often, the criminal already has some personal information on you, including your account or credit card numbers. That can create a false sense of security. The call came from a VoIP account as well.

Vishing, as you might imagine from these scams, has some advantages over traditional phishing tricks.

First, VoIP service is fairly inexpensive, especially for long distance, making it cheap to make fake calls. Second, because it's web-based, criminals can use software programs to create phony automated customer service lines.

But if the thieves are giving out their phone numbers, they should be easy to track, right? Wrong. Criminals can mask the number they are calling from, thwarting caller ID. And in some cases, the VoIP number belongs to a legitimate subscriber whose service is being hacked.

So how prevalent is vishing? Hard to say, due to reporting difficulties. "A lot of would-be victims are reporting this as SPAM or phishing," says Dan Larkin, Chief of the FBI's Cyber Initiative and Resource Fusion Unit. "But we know it's out there. Its happening."

Don't let it happen to you. Larkin recommends greeting a phone call or e-mail seeking personal information with a healthy dose of skepticism. If you think the call is legit, you can always hang up and call back using the customer service number provided by the financial institution when the account was opened. And please contact the Internet crime Complaint Center on 1-800-878-3256 if you think you were either a vishing victim or received a suspicious call or e-mail.

WE'VE MOVED!

USNRC

Office of the Inspector General

11555 Rockville Pike

Mail Stop O 5E13

Rockville, MD 20852

HOTLINE NUMBER

1-800-233-3497

TDD LINE

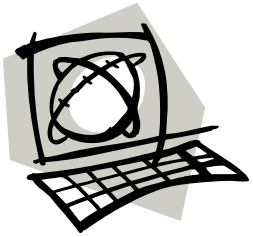
1-800-270-2787

Internet Crime—The Latest Numbers

http://www.fbi.gov/page2/march07/ic3031607.htm

When it comes to crime, the Internet is like a Swiss Army knife—a multi-purpose tool that's easy to use and highly versatile. That's made crystal clear by the 2006 annual report just issued by the Internet Crime Complaint Center (IC3), which shows how criminals used the 'Net to launch nine different varieties of fraud alone. **Overall totals:** During 2006, consumers filed 207,492 complaints. Complainants said they lost $198.4 million, the highest total ever.

Types of fraud: Nearly 45 percent of the complaints involved online auction fraud—such as getting a different product than you expected—making it the largest category; more than 19 percent concerned undelivered merchandise or payments.



The perpetrators: Three-quarters were men. Nearly 61 percent lived in the U.S., with half in one of seven states. Other top countries included the U.K., Nigeria, Canada, Romania, and Italy.

Victims: All over the map. But the report shows that the "average" complainant was a man between 30 and 40 living in California, Texas, Florida, or New York. Individuals who reported losing money lost an average of $724; the highest losses involved Nigerian letter fraud, with a median loss of $5,100. Nearly 74 percent of the complaints said they were contacted through e-mail, and 36 percent complained of fraud through websites, highlighting the anonymous nature of the web.

GREETING CARD SCAM

There continue to be reports of Internet fraud related to electronic greeting cards containing malware (malicious software). The cards, which are also referred to as e-cards or postcards, are being sent via spam.

Like many other Internet fraud schemes, the perpetrators claim the card is from a family member or friend. Although there have been variations in the spam message and attached malware, generally the spam directs the recipient to click the link provided in the e-mail to view their e-card. Upon clicking the link, the recipient is unknowingly taken to a malicious web page.

Beware of unsolicited e-mails. It is recommended not to open e-mails from unknown senders because they often contain viruses or other malicious software.