UNITED STATES NUCLEAR REGULATORY COMMISSION

OIG INFORMATION DIGEST

Volume 2, Number 1
NUREG/BR-0304 May 2004

TO TELL OR NOT TO TELL

This issue of the *OIG Information Digest* is intended to make new and veteran NRC employees more aware of the problems that can be encountered when working with sensitive unclassified information. There have been occasions in the past few years when sensitive NRC information has been released to the public. It is important that you, as a Government employee, are aware of what types of information you are obligated to disclose and which types must be protected.

Prohibited Disclosure

The following are the types of information that should not be divulged to those without a need to know. The NRC handles three types of sensitive unclassified information:

Safeguards Information (SGI) concerns the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material.

Proprietary information (PROPIN) concerns trade secrets, commercial, and financial information.

Official Use Only (OUO) information concerns agency records, privacy data, and investigative reports.

Be mindful of the avenues through which sensitive information can be inadvertently released:

- E-mails
- Agencywide Documents Access and Management System (ADAMS)
- Telephone conversations
- Unattended computer terminals with sensitive information on the screen
- Documents released through the Freedom of Information Act (FOIA) process
- The mail
- Discussion of sensitive information in public meetings or public places
- Documents left on printers or in the copy machine
- Documents left on a desk
- Unsecured floppy disks
- Improperly disposed information in a recycle box
- Unsecured safes
- Shared computer passwords

OIG has received many allegations and has conducted 14 investigations in the recent past relating to the inadvertent release of safeguards information, information through the FOIA, classified information, and official use only information.

However, in each case, these releases were deemed not to be deliberate and willful acts.

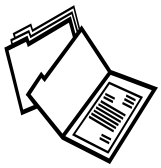
Inside this issue:

OIG AUDIT REPORTS

OIG Audit Reports Continue to Focus on Preventing Inappropriate Release of Information

Preventing the inadvertent release of sensitive NRC information to the public has been an ongoing concern for NRC in recent years. Examples of such releases, while not frequent, have occurred often enough to indicate that prevention demands an ongoing, rigorous effort by the agency to keep employees aware of their responsibilities and to review and improve procedures for protecting this information.

Since 1999, the Office of the Inspector General has issued four audit reports specifically addressing the need to protect sensitive agency information from inadvertent release to the public. Some themes in these reports reflect the need to provide training, consolidate and clarify guidance, and maintain records of inadvertent releases so that trends can be identified. The reports described instances where information was inadvertently released to the public.



Examples included the inappropriate:

- Release of names and identifying information in two Freedom of Information Act (FOIA) responses resulting in legal action against NRC.

- Release through ADAMS of more than 700 non-public documents which included proprietary information submitted by licensees and personal information such as employee social security numbers and birth dates.

- Release of an Official Use Only (OUO) preliminary draft of the Yucca Mountain Review Plan.

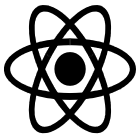
- Distribution of documents including safeguards information (SGI) pertaining to NRC's force-on-force security testing program.

- Verbal disclosure of SGI pertaining to the force-on-force program during an industry-sponsored meeting.

One of these audits was initiated in response to a congressional request, one was in response to a request from the NRC Chairman, and two were initiated by OIG. The following are summaries of these four audit reports, beginning with the most recent.

OIG-04-A-04, *Audit of NRC's Protection of Safeguards Information* (January 8, 2004)

This audit sought to determine whether NRC adequately defines SGI, prevents the inappropriate release of SGI to anyone who should not have access to it, and ensures the protection of SGI. SGI deals with information related to the physical protection of operating power reactors, spent fuel shipments, or the physical protection of special nuclear material. SGI is to be protected in accordance with NRC's sensitive unclassified information security program. In accordance with NRC Management Directive and Handbook 12.6, "NRC Sensitive Unclassified Information Security Program," SGI must be communicated over secure telecommunications equipment, not be processed on the local area network, be properly marked, and include a cover sheet to facilitate its recognition.



OIG found that NRC's program to protect SGI had three weaknesses: (1) The benefit of the SGI designation as sensitive unclassified information was not clear, (2) NRC and licensee representatives had inappropriately released SGI to unauthorized individuals because of handling errors and differing interpretation of what constitutes SGI, and (3) NRC lacked a central authority for controlling, coordinating, and communicating SGI program requirements.

OIG-03-A-01, *Review of NRC's Handling and Marking of Sensitive Unclassified Information* (October 16, 2002)

The objective of this review was to assess NRC's program for the handling, marking, and protection of OUO information. OUO is one category of sensitive unclassified information that includes personnel records, privacy data, investigative reports, and predecisional or internal

OIG AUDIT REPORTS (con't from page 2)

NRC data. This category of information requires special handling to ensure only limited internal distribution and no disclosure to the public. Some OUO information is intended to be released to the public after certain conditions have been met such as official approval of the document.

OIG found that NRC's guidance for protecting OUO documents from inadvertent public release was inadequate. Specifically, the use of OUO cover sheets was left to the discretion of the document originator. In addition, individual pages of documents were not always marked and were therefore vulnerable to public disclosure if separated from the cover sheet. Consistent markings were not used on sensitive unclassified documents that were marked, which added to the confusion surrounding the proper marking and handling of sensitive unclassified information. Auditors also found that many employees were not knowledgeable about NRC's guidance and requirements in this area because training on handling, marking, and protecting sensitive unclassified information was not provided to all NRC employees and contractors on a regular basis.

OIG-01-A-16, *Review of the Unauthorized Release of Documents to the ADAMS Public Library*, (September 24, 2001)

The objective of this review was to assess the cause of an unauthorized release of non-public information to the Agencywide Documents Access and Management System (ADAMS) public library. ADAMS is NRC's electronic record keeping system that maintains the official records of the agency. ADAMS is also NRC's public information dissemination system that places publicly available records on NRC's public Web server. The ADAMS Public Library contains duplicate copies of publicly available official agency records copied from the ADAMS Main Library.

The audit found that ADAMS software controls were inadequate to prevent the unauthorized release of documents, the ADAMS security plan did not entirely identify risks to the system and was not finalized, and communication was ineffective subsequent to the unauthorized release of non-public documents.

OIG/98A, *Review of NRC Controls To Prevent the Inadvertent Release of Sensitive Information* (February 2, 1999)

This audit sought to determine if NRC's management controls for protecting sensitive information from inadvertent release were adequate and whether NRC was implementing the agency's guidance to protect this information from inadvertent release. The audit also sought to determine if the ADAMS development process was taking into consideration the need to protect sensitive data from unauthorized release.

The audit found that NRC's guidance and policies concerning sensitive information were scattered among many management directives, manuals, and other documents. This increased the potential for staff to miss or misapply pertinent guidance and that inadvertent releases of sensitive information occur because staff have varied levels of training and awareness regarding the handling of this information.

Agency Actions in Response to OIG Audits

Each of these audit reports contained recommendations to NRC for strengthening controls to protect sensitive information from inadvertent release. Some changes that NRC has implemented as a result of these recommendations include:

- Redesign of OUO and SGI cover sheets to clearly illustrate and explain required document markings and access requirements.
- Revision of several management directives to clarify agency guidance concerning OUO protection.
- Revision of ADAMS operating procedures to adequately control the process for copying documents from the Main Library to the Public Library.

OIG AUDIT REPORTS (Cont. from page 3)

- Mandatory annual employee training concerning the protection of sensitive unclassified information.

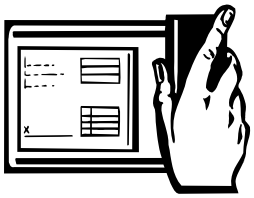
- Improved cross-referencing of management directives to facilitate employee awareness of agency guidance concerning the protection of sensitive information.

CREDIT REPAIR SCAM (Article from the National Consumer's League)

In the last issue of the *OIG Information Digest*, we provided information concerning identity theft. A lesser known scam that is targeting individuals across the country is referred to as the credit repair scam. This scam involves people that currently have a problem with their credit ratings or have had problems in the past.

The Scam

Everyday, companies nationwide appeal to consumers with poor credit histories. They promise, for a fee, to clean up your credit report so you can get a car loan, a home mortgage, insurance, or even a job. The truth is, they can't deliver. After you pay them hundreds or thousands of dollars in up-front fees, these companies do nothing to improve your credit report; many simply vanish with your money .



The following tips are intended to help you avoid falling victim to this type of scam:

No one can erase negative information if it's accurate. Only incorrect information can be removed. Accurate information stays on your record for 7 years from the time it's reported (10 years for bankruptcy). Even information about bills you fell behind on but now are paid will remain on your report for these time periods.

Credit repair services can't ask for payment until they've kept their promises. Federal law also requires credit repair services to give you an explanation of your legal rights, a detailed written contract, and 3 days to cancel (this applies to for-profit services, not to nonprofit organizations, banks and credit unions, or the creditors themselves).

You can correct mistakes on your credit report yourself. If you were recently denied credit because of information in your credit report, you have the right to request a copy. There may be a small fee, if your State law does not provide for one free report a year. However, it doesn't cost anything to question or dispute items in your report. Follow the instructions provided by the credit bureau. The major credit bureaus are:
Equifax, 800-685-111, *www.equifax.com*;
Experian, 800-682-7654, *www.experian.com*; and
Trans Union, 800-916-8800, *www.transunion.com*. Contact all three, as the information each has may vary.

You can add an explanation to your report. If there is a good reason why you weren't able to pay bills on time (job loss, sudden illness, etc.) or you refused to pay for something because of a legitimate dispute, give the credit bureau a short statement to include in your file.

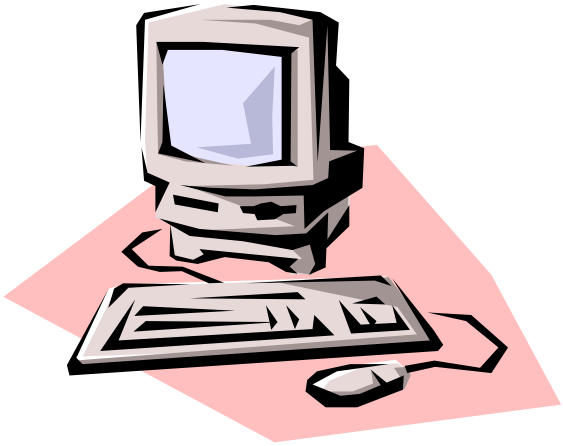
Organization

UNITED STATES NUCLEAR REGULATORY COMMISSION

Office of the Inspector General
11545 Rockville Pike
Mail Stop T 5D28
Rockville, MD 20851

Hotline: 800-233-3497
Fax: 301-415-5091

We're on the Web!!



CREDIT REPAIR SCAM (cont. from page 4)

Know that you can't create a second credit file. Fraudulent companies sometimes offer to provide consumers with different tax identification or social security numbers in order to create a new credit file. This practice, called "file segregation," is illegal, and doesn't work.

If you have credit problems, get counseling. Your local Consumer Credit Counseling Service (CCCS) can provide advice about how to build a good credit record. The CCCS may also be able to make payment plans with your creditors if you've fallen behind. These services are offered for free or at a very low cost. To find the nearest CCCS office, call toll-free, 800-388-2227, or go to *www.nfcc.org*.

As an NRC employee, you are entitled help from the NRC Employee Assistance Program (EAP). There are benefits provided by the EAP if you are experiencing financial difficulties and do not know who to turn to for help. The EAP will provide assessment, referral, and short-term problem resolution for a number of personal and worksite-based issues. Employees who are experiencing financial problems are referred to local credit counseling agencies.

All inquiries and services to the EAP are kept confidential within the law and all records are protected by law (42 CFR Part 2).