NRC Yellow Announcement

UNITED STATES
NUCLEAR REGULATORY COMMISSION

Announcement No. 024

Date: April 14, 2004

To: All NRC Employees

SUBJECT: NO COMMENT POLICY FOR CLASSIFIED AND SAFEGUARDS INFORMATION

The purpose of this announcement is to reinforce the policy, procedures, and guidance for NRC personnel and contractors concerning classified and Safeguards Information (SGI). This announcement addresses information in the public domain.

Classified information and SGI are protected by preventing dissemination to unauthorized individuals. Occasionally, such information appears in the public domain without authorization. Commenting on the information or attempting to prevent its further dissemination could result in greater damage to the national security and/or common defense and security of the United States than if no comment is made about the information.

The fact that information has appeared publicly does not render the information unclassified or decontrolled. If the discussion concerns protected security information, the answer to questions raised about the accuracy, designation or classification, or technical merit of such information should be "no comment." A follow up statement should be "The NRC neither confirms nor denies the presence or accuracy of protected information in the public domain."

Documents containing speculation in a subject area involving protected security information by individuals not authorized for access to such information are sometimes submitted for unsolicited review by NRC or its contractors. Again, no comment should be made on the accuracy, designation or classification, or technical merit of the documents. Any decision by management to comment shall be made, insofar as possible, in coordination with other pertinent NRC offices (e.g., OGC, OPA, NSIR) and with due consideration of the possible ramifications of an NRC comment.

If there is any doubt as to the appropriate action to take when implementing this policy, the Information Security Section, NSIR, should be consulted at 301-415-2212. This policy will be incorporated into final versions of NRC Management Directives 12.2 and 12.6, which are currently being updated.

/RA/

Roy P. Zimmerman, Director
Office of Nuclear Security
and Incident Response

Management Directive Reference: Management Directives 12.2 and 12.6

NRC Yellow Announcements Index

C-14

NRC Announcement

November 2, 2004 - Policy Reminder: Protection of TSA's Sensitive Security Information

The Transportation Security Administration (TSA) recently published a rule (49 CFR Part 1520) that revises, among other things, the protection requirements for a category of information known as "Sensitive Security Information (SSI)." SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would be detrimental to the security of transportation. The NRC may receive SSI during the course of business. The TSA rule states in part that SSI, when not in physical possession by an authorized person, must be stored in a secure container, such as a locked desk or a file cabinet or in a locked room. The rule further states that only persons with a need-to-know may have access to SSI. Presently, NRC Management Directive (MD) 12.6, "NRC Sensitive Unclassified Information Security Program," allows NRC employees and its contractors to openly store sensitive unclassified information (SUI) (i.e., proprietary or official use only, not Safeguards Information) within NRC space provided that electronic access controls are present or guards are on duty. TSA has determined that the sensitivity of SSI warrants its storage in a locked desk or equivalent even if guards or electronic access controls are in place. Therefore, to comply with current TSA requirements, all recipients or holders of SSI are reminded that such information must be stored in a locked drawer, cabinet, or behind a locked door when not in use.

If you have any further questions regarding the protection of SSI or any other form of SUI that is not covered by MD 12.6, please contact the Information Security Section at 415-2212.

Distribution: Headquarters, Regions

Announcements by Date | Announcements by Category

Back