NUREG/BR-0168, Rev. 3

GUIDE FOR INFORMATION TECHNOLOGY SECURITY

# Policy for Processing Unclassified Safeguards Information (SGI) on NRC Computers

U.S. Nuclear Regulatory Commission
Office of the Chief Information Officer

**Unauthorized reproduction of copyrighted software is against the law**

## Policy for Processing Unclassified Safeguards Information (SGI) on NRC Computers

Safeguards information (SGI) is sensitive unclassified information about the security measures for the physical protection of special nuclear material, source material, byproduct material, and production and utilization facilities. Under NRC regulations, SGI must be protected and unauthorized disclosures of SGI are subject to civil and criminal sanctions.

The protective measures required for SGI are similar to those required for classified data at the confidential level. SGI may be stored, processed or produced **only** on a stand-alone personal computer (PC)–that is, a PC not physically or in any other way connected to the NRC or any other unclassified network. The stand-alone PC unit must have a removable storage medium with a bootable operating system. The bootable operating system must be used to load and initialize the computer. The removable storage medium must also contain the software application programs, and all data must be processed and saved on the same removable storage medium. A mobile device (such as a laptop computer) may also be used for the automated processing of SGI provided the device is secured in an appropriate storage container when not in use.

If a stand-alone or mobile personal computer has a removable drive, the operating system and the applications and data used for SGI processing must **all** reside on the same removable drive. The removable hard drive must be secured in an approved security container when not in use. SGI files may be transmitted across an unclassified network (e.g., a network not approved for the transmission of classified data), only if they have first been properly encrypted using encryption algorithms approved by the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA). Contact the Computer Security Staff (CSS) in the Office of the Chief Information Officer (OCIO) for assistance in identifying approved methods

of encryption. The OCIO CSS phone number is (301) 415-7430.

The following procedures apply equally to a PC or mobile device (computer) and ***must*** be used in handling and processing SGI. For more details, see MD 12.5, "NRC Automated Information Security Program."

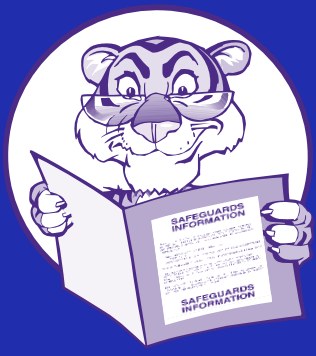
- For each unit, a system security plan ***must*** be prepared and approved by the OCIO and an information system security officer (ISSO) ***must*** be appointed.
- The computer ***must*** not use a fixed hard disk for storing any data (intermediate results, final results, overflow, or backup) unless the computer can be provided with adequate security for the open storage of SGI. The security plan ***must*** specify that the hard drive be sanitized or destroyed before the computer is removed from the protected area.
- Any computer not located in an NRC-sensitive compartmented information facility (SCIF) or another facility approved by the Division of Facilities and Security (DFS) ***must*** be physically disconnected from LANs, modems, and shared printers.
- Unauthorized personnel ***must not*** be allowed to see the information being processed. Monitors and printers may be protected by screens or hoods, or placed so they face away from door ways, windows, or open areas.
- The computer ***must*** be attended at all times when processing SGI.
- All media (e.g., diskettes, tapes, printouts) ***must*** be properly marked and stored in DFS-approved storage containers when not in use, in accordance with MD 12.6, "NRC Sensitive Unclassified Information Security Program."
- Disks, diskettes, ribbons, and printouts ***must*** be disposed of in accordance with MD 12.5 and MD 12.6.

## Scan software, disk, and files for computer viruses

- SGI data can be disposed of by (1) destroying the electronic storage medium, (2) using an approved software product such as BCWIPE or SDELETE to obliterate the sensitive data, or (3) degaussing (demagnetizing) the disk to erase all data. Questions about how to destroy SGI data on an electronic storage medium should be referred to the OCIO CSS .
- Documents containing SGI or other sensitive unclassified information ***must*** not be left unattended. This applies particularly to printers because print jobs are often easily forgotten.
- Portable mass storage devices (PMSD) are not to be used to store SGI data. These storage include flash memory storage such as USB thumb drives and compact flash.
- Upon receiving an e-mail message containing an encrypted SGI document, save the SGI file to a removable medium (diskette, CD, Zip drive, Bernoulli box, or other removable hard drive). Enter the full path and filename for the document (e.g., a:\SGI_MSG). After saving the document, delete the e-mail.
- Encryption passwords should never be written down anywhere; they should be committed to memory. But remember: if you forget the required password, the ability to access or retrieve the document will be lost.

The computer user is responsible for assessing the sensitivity and ensuring the security of the data. Users ***must*** be alert to possible breaches in security and ***must*** follow NRC's security regulations.

Questions about the contents of this publication or any other computer security issue should be referred to the OCIO CSS at (301) 415-7430.




NRC FORM 461
(3-2003)

SAFEGUARDS INFORMATION

U.S. NUCLEAR REGULATORY COMMISSION

THIS DOCUMENT CONTAINS INFORMATION
BE PROTECTED FROM UNAUTHORIZED
ACCORDANCE WITH THE FOLLOWING
THAT APPLY:

NRC MANAGEMENT
10 CFR 73.21
SECTION 147,