OMB Control No.: 3150-0002

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-0001

August 28, 2002

NRC REGULATORY ISSUE SUMMARY 2002-15
NRC APPROVAL OF COMMERCIAL DATA ENCRYPTION SYSTEMS FOR THE ELECTRONIC TRANSMISSION OF SAFEGUARDS INFORMATION

ADDRESSEES

All authorized recipients and holders of sensitive unclassified safeguards information (SGI).

INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing this regulatory issue summary (RIS) to provide guidance to addressees on obtaining NRC approval of commercial data encryption systems for the electronic transmission of SGI. This RIS requires no action or written response on the part of addressees.

BACKGROUND

"Sensitive unclassified information" is defined by Public Law 100-235. The primary authorities for the protection of sensitive unclassified information include the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and Parts 2 and 9 of Title 10 of the *Code of Federal Regulations* (10 CFR Parts 2 and 9). The unauthorized disclosure of SGI — a type of sensitive unclassified information — is prohibited under the provisions of Section 147 of the Atomic Energy Act of 1954, as amended, and 10 CFR 73.21. Additional guidance on protecting SGI can be found in NUREG-0794, "Protection of Unclassified Safeguards Information (Criteria and Guidance)," dated October 1981.

NRC regulations in 10 CFR 73.21(g)(3) state that except under emergency or extraordinary conditions, SGI shall be transmitted only by protected telecommunications circuits (including facsimile) approved by the NRC, and physical security events that are required to be reported pursuant to 10 CFR 73.71 are considered to be extraordinary conditions. In addition, 10 CFR 73.21(h) states that SGI may be processed or produced on an automatic data processing (ADP) system, provided that the system is self-contained within the authorized holder's facility and requires the use of an entry code for access to stored information; other systems may be used if approved for security by the NRC.

The National Institute of Standards and Technology (NIST) has established the Cryptographic Module Validation Program (CMVP), which validates conformance of cryptographic modules to the Security Requirements for Cryptographic Modules in Federal Information Processing Standard (FIPS) 140-1 and FIPS 140-2 and, as appropriate, any other FIPS cryptography standard.

ML022400435

C-17

The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 and 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive unclassified information. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the acceptance testing of cryptographic modules conducted by accredited testing laboratories. There are currently four laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP), which perform compliance testing in accordance with FIPS 140-1 and 140-2; three are in the United States and one is in Canada. The Secretary of Commerce has made FIPS 140-1 and 140-2 mandatory and binding for U.S. Federal agencies and organizations. This is specifically applicable when a Federal agency determines that cryptography is necessary to protect sensitive unclassified information.

SUMMARY OF ISSUE

The following guidance is provided to addressees who voluntarily choose to transmit SGI in electronic format:

(1) Select a commercially available encryption system that NIST has validated as conforming to FIPS 140-1 and 140-2. Additional information on NIST-approved encryption systems can be found at http://csrc.nist.gov/pki/nist_crypto/welcome.html. NIST maintains a current listing of all validated encryption systems at http://csrc.nist.gov/cryptval/140-1/1401val.htm.

(2) Submit a written request for NRC approval to use the selected commercially available encryption system as required by 10 CFR 73.21(g)(3).

(3) General performance requirements for the protection of safeguards information, found at 10 CFR 73.21(a), state that "each licensee... and each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure. To meet this general performance requirement, licensees and persons subject to [10 CFR 73.21] shall establish and maintain an information protection system that includes the measures specified in paragraphs (b) through (i) of [10 CFR 73.21]. Information protection procedures employed by State and local police forces are deemed to meet these requirements."

Therefore, in accordance with 10 CFR 73.21(a), licensees and persons who produce, receive, or acquire Safeguards Information should prepare written procedures that address how applicable provisions of 10 CFR 73.21 will be met and how the selected encryption system will be used. Written procedures should include, but are not limited to, access controls; where and when encrypted communications can be made; how encryption keys, codes, and passwords will be protected from compromise; actions to be taken if the encryption keys, codes, or passwords are, or are suspected to have been, compromised (for example, notification of all authorized users); and how the identity and access authorization of the recipient will be verified.

(4) NRC approval to use a commercially available encryption system is contingent upon NIST approval. If an encryption system no longer satisfies FIPS 140-1 and 140-2 and is removed from the list of NIST-approved encryption systems, NRC approval that was previously granted is automatically withdrawn and affected addressees must discontinue

using that encryption system. It is the responsibility of the authorized recipient or holder of SGI to verify — prior to each use — that its encryption system continues to have NIST approval.

(5) The guidance contained in this RIS does not alter or revise any current regulatory requirements for the protection of SGI. For addressees who choose not to transmit SGI in electronic format, 10 CFR 73.21(g)(1) and (2) will continue to apply.

(6) The NRC is evaluating the feasibility of employing electronic data encryption for the transmission of SGI between authorized holders and the NRC. Pending a decision on this matter, 10 CFR 73.21(g)(1) and (2) will continue to apply when SGI is transmitted between addressees and the NRC.

BACKFIT DISCUSSION

This RIS does not require any action or written response and does not require any modification to plant structures, systems, components, or facility design. Therefore, the NRC staff did not perform a backfit analysis.

FEDERAL REGISTER NOTIFICATION

The NRC did not publish a notice of opportunity for public comment in the *Federal Register* because this RIS is informational and pertains to a matter that does not represent a departure from current regulatory requirements and practice.

PAPERWORK REDUCTION ACT STATEMENT

This RIS contains information collections that pose an insignificant burden to respondents to request approval of an encryption system and prepare written procedures for safeguarding the transmitted information. The public burden for this information collection is estimated to average 2 hours per request. Because the burden for this information collection is insignificant, Office of Management and Budge (OMB) clearance is not required. Existing requirements were approved by OMB, approval number 3150-0002.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

If you have any questions about this matter, please contact the person listed below or the appropriate NRC project manager.

/RA/
Robert C. Pierson, Director
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

/RA/
William D. Beckner, Program Director
Operating Reactor Improvements Program
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

Technical contacts: Nancy Fontaine, NSIR
301-415-1253
Email: nrf@nrc.gov

Melvyn Leach, NMSS
301-415-7836
Email: mnl@nrc.gov

Attachment: List of Recently Issued Regulatory Issue Summaries