

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS
WASHINGTON, DC 20555-0001

January 26, 2006

**NRC REGULATORY ISSUE SUMMARY 2002-15, REVISION 1
NRC APPROVAL OF COMMERCIAL DATA ENCRYPTION PRODUCTS
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 re-issuing this Regulatory Issue Summary (RIS) to correct and clarify RIS 2002-15, "NRC Approval of Commercial Data Encryption Systems for the Electronic Transmission of Safeguards Information [SGI]," which was issued to provide guidance to addressees on obtaining NRC approval of commercial data encryption products for the electronic transmission of SGI. This RIS requires no action or written response on the part of addressees. This revision supercedes in its entirety, the guidance provided in the original RIS.

BACKGROUND INFORMATION

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 circuits) approved by the NRC and that physical security events 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 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) established a Cryptographic Module Validation Program (CMVP) that validates conformance of cryptographic modules to Security Requirements for Cryptographic Modules in Federal Information Processing Standard (FIPS) 140-1 or FIPS 140-2 and, as appropriate, to any other FIPS cryptography standard.

ML050460031

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 or 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive unclassified information. Computer Security Division of NIST and CSE jointly serve as the validation authorities for the acceptance testing of cryptographic modules by accredited testing laboratories. Currently, nine laboratories are accredited by the National Voluntary Laboratory Accreditation Program, to perform compliance testing in accordance with FIPS 140-1 or 140-2; five are in the United States, two are in Canada, and two are in the United Kingdom. The Secretary of Commerce has made the use of either FIPS 140-1 or 140-2 mandatory and binding for U.S. Federal agencies and organizations. This requirement 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 desire to transmit SGI in electronic format:

- (1) Select a commercially available encryption product that uses a cryptographic module validated to NIST 140-1 or 140-2 standards. Additional information on NIST-validated encryption products is posted on the NIST web site at http://csrc.nist.gov/pki/nist_crypto/welcome.html. NIST maintains a current listing of all validated encryption products at <http://csrc.nist.gov/cryptval/140-1/1401val.htm>.
- (2) Submit a written request, including FIPS validation certificate for cryptographic module, to the NRC for approval to use the selected commercially available encryption product, as required by 10 CFR 73.21(g)(3). Include a copy of the FIPS validation certificate of the selected encryption product.
- (3) Use FIPS-approved cryptographic algorithms to encrypt data for electronic transmission.
- (4) Check the NIST web site to ensure that the cryptographic algorithms selected for encrypting data are still approved by NIST before use. The NRC approves only NIST-approved cryptographic algorithms. Thus, if NIST no longer approves a cryptographic algorithm, the NRC no longer accepts it.
- (5) Addressees may replace the current version of encryption products that were approved by the NRC with a newer version of encryption product without prior approval from the NRC, provided that the addressees document that the newer version of encryption product uses the same cryptographic module as the current version of encryption product, i.e., document that the FIPS validation certificate of the new version of encryption product is the same as the current version of encryption product.
- (6) General performance requirements for the protection of SGI 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 this section shall establish and maintain an information protection product that includes the measures specified in paragraphs (b) through (i) of this section. Information protection procedures employed by State and local police forces are deemed to meet these requirements.” Therefore, licensees and persons who produce, receive, or acquire SGI should prepare written procedures that address how applicable provisions of 10 CFR 73.21 will be met and how the selected encryption product will be used. The 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.

- (7) 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.
- (8) 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 does not depart from current regulatory requirements and practice.

SMALL BUSINESS REGULATORY ENFORCEMENT FAIRNESS ACT of 1996

The NRC has determined that this action is not subject to the Small Business Regulatory Enforcement Fairness Act of 1996.

PAPERWORK REDUCTION ACT STATEMENT

This RIS contains information collections that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collections were approved by the Office of Management and Budget, approval number 3150-0011, which expires February 28, 2007. The burden to the public for these (voluntary/mandatory) information collections is estimated to average 0.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the

information collection. Send comments regarding this burden estimate or any other aspect of these information collections, including suggestions for reducing the burden, to the Records and FOIA/Privacy Services Branch (T-5 F53), U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, or by Internet electronic mail to INFCOLLECTS@NRC.GOV; and to the Desk Officer, Office of Information and Regulatory Affairs, NEOB-10202, (3150-0011), Office of Management and Budget, Washington, DC 20503.

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 Office of Management and Budget control number.

CONTACT

Please direct any questions about this matter to the technical contact listed below, or to the appropriate Office of Nuclear Reactor Regulation project manager.

/RA/
Charles L. Miller, Director
Division of Industrial
and Medical Nuclear Safety
Office of Nuclear Material Safety
and Safeguards

/RA/
Christopher I. Grimes, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

Technical Contact: Eric Lee, NSIR
301-415-8099
E-mail: exl@nrc.gov

Enclosure: Recently Issued NMSS Generic Communications

Note: NRC generic communications may be found on the NRC public Web site, <http://www.nrc.gov>, under Electronic Reading Room/Document Collections.

Recently Issued NMSS Generic Communications

Date	GC No.	Subject	Addressees
2/11/05	BL-05-01	Material Control and Accounting at Reactors and Wet Spent Fuel Storage Facilities	All holders of operating licenses for nuclear power reactors, decommissioning nuclear power reactor sites storing spent fuel in a pool, and wet spent fuel storage sites.
01/13/06	RIS-05-27, Rev. 1	NRC Regulatory Issue Summary 2005-27, Rev. 1, NRC Timeliness Goals, Prioritization of Incoming License Applications and Voluntary Submittal of Schedule for Future Actions for NRC Review	All 10 CFR Parts 71 and 72 licensees and certificate holders.
12/22/05	RIS-05-31	Control of Security-related Sensitive Unclassified Non-safeguards Information Handled by Individuals, Firms, and Entities Subject to NRC Regulation of the Use of Source, Byproduct, and Special Nuclear Material	All licensees, certificate holders, applicants, and other entities subject to regulation by the U.S. Nuclear Regulatory Commission of the use of source, byproduct, and special nuclear material, except for those as covered by provisions of Regulatory Issue Summary (RIS) 2005-26 for nuclear power reactors.
11/23/05	RIS-05-24	Control of Radiation Dose to Visitors of Hospital Patients	All medical licensees.
11/14/05	RIS-05-21	Clarification of the Reporting Requirements in 10 CFR 20.2201	All U.S. Nuclear Regulatory Commission licensees and Part 76 certificate holders authorized to possess licensed material.
11/08/05	RIS-05-27	NRC Timeliness Goals, Prioritization of Incoming License Applications and Voluntary Submittal of Schedule for Future Actions for NRC Review	All 10 CFR Parts 71 and 72 licensees and certificate holders.
10/28/05	RIS-05-22	Requirements for the Physical Protection During Transportation of Special Nuclear Material of Moderate and Low Strategic Significance: 10 CFR Part 72 vs. Regulatory Guide 5.59 (1983)	All holders of licenses for the possession of special nuclear material (SNM) that ship Category II and III quantities of this material.
10/07/05	RIS-05-23	Clarification of the Physical Presence Requirement During Gamma Stereotactic Radiosurgery Treatments	All gamma stereotactic radiosurgery (GSR) licensees.
09/27/05	RIS-04-17, Rev. 1	Revised Decay-in-Storage Provisions for the Storage of Radioactive Waste Containing Byproduct Material	All licensees regulated under 10 CFR Parts 30, 32, 33, 35, 39, and 50.

Date	GC No.	Subject	Addressees
08/25/05	RIS-05-18	Guidance for Establishing and Maintaining a Safety Conscious Work Environment	All licensees, applicants for licenses, holders of certificates of compliance, and their contractors subject to NRC authority
08/10/05	RIS-05-16	Issuance of NRC Management Directive 8.17, "Licensee Complaints Against NRC Employees"	All licensees and certificate holders.
08/03/05	RIS-05-15	Reporting Requirements for Damaged Industrial Radiographic Equipment	All material licensees possessing industrial radiographic equipment, regulated under 10 CFR Part 34.
07/13/05	RIS-05-13	NRC Incident Response and the National Response Plan	All licensees and certificate holders.
07/11/05	RIS-05-12	Transportation of Radioactive Material Quantities of Concern NRC Threat Advisory and Protective Measures System	Licensees authorized to possess radioactive material that equals or exceeds the threshold values in the Additional Security Measures (ASM) for transportation of Radioactive Material Quantities of Concern (RAMQC) under their 10 CFR Part 30, 32, 50, 70, and 71 licenses and Agreement State licensees similarly authorized to possess such material in such quantities under their Agreement State licenses.
07/11/05	RIS-05-11	Requirements for Power Reactor Licensees in Possession of Devices Subject to the General License Requirements of 10 CFR 31.5	All holders of operating licenses for nuclear power reactors and generally licensed device vendors.
06/10/05	RIS-05-10	Performance-Based Approach for Associated Equipment in 10 CFR 34.20	All industrial radiography licensees and manufacturers and distributors of industrial radiography equipment.
04/18/05	RIS-05-06	Reporting Requirements for Gauges Damaged at Temporary Job Sites	All material licensees possessing portable gauges, regulated under 10 CFR Part 30.
04/14/05	RIS-05-04	Guidance on the Protection of Unattended Openings that Intersect a Security Boundary or Area	All holders of operating licenses or construction permits for nuclear power reactors, research and test reactors, decommissioning reactors with fuel on site, Category 1 fuel cycle facilities, critical mass facilities, uranium conversion facility, independent spent fuel storage installations, gaseous diffusion plants, and certain other material licensees.

Date	GC No.	Subject	Addressees
02/28/05	RIS-05-03	10 CFR Part 40 Exemptions for Uranium Contained in Aircraft Counterweights - Storage and Repair	All persons possessing aircraft counterweights containing uranium under the exemption in 10 CFR 40.13(c)(5).
12/23/05	IN-05-32	Product Alert for Fire Hydrants	All holders of operating licenses for nuclear power reactors and fuel cycle facilities, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.
11/17/05	IN-05-31	Potential Non-conservative Error in Preparing Problem-dependent Cross Sections for use with the KENO V.a or KENO-VI Criticality Code	All licensees using the KENO V.a or KENO-VI criticality code module in Version 5 of the Standardized Computer Analyses for Licensing Evaluation (SCALE) software developed by Oak Ridge National Laboratory (ORNL).
10/31/05	IN-05-28	Inadequate Test Procedure Fails to Detect Inoperable Criticality Accident Alarm Horns	All licensees authorized to possess a critical mass of special nuclear material.
10/07/05	IN-05-27	Low Dose-Rate Manual Brachytherapy Equipment Related Medical Events	All medical licensees.
07/29/05	IN-05-22	Inadequate Criticality Safety Analysis of Ventilation Systems at Fuel Cycle Facilities	All licensees authorized to possess a critical mass of special nuclear material.
06/23/05	IN-05-17	Manual Brachytherapy Source Jamming	All medical licensees authorized to possess a Mick applicator.
05/17/05	IN-05-13	Potential Non-conservative Error in Modeling Geometric Regions in the Keno-v.a Criticality Code	All licensees using the Keno-V.a criticality code module in Standardized Computer Analyses for Licensing Evaluation (SCALE) software developed by Oak Ridge National Laboratory (ORNL)
05/17/05	IN-05-12	Excessively Large Criticality Safety Limits Fail to Provide Double Contingency at Fuel Cycle Facility	All licensees authorized to possess a critical mass of special nuclear material.
04/07/05	IN-05-10	Changes to 10 CFR Part 71 Packages	All 10 CFR Part 71 licensees and certificate holders.
040/01/05	IN-05-07	Results of HEMYC Electrical Raceway Fire Barrier System Full Scale Fire Testing	All holders of operating licenses for nuclear power reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel, and fuel facilities licensees.

Date	GC No.	Subject	Addressees
03/10/05	IN-05-05	Improving Material Control and Accountability Interface with Criticality Safety Activities at Fuel Cycle Facilities	All licensees authorized to possess a critical mass of special nuclear material.

Note: NRC generic communications may be found on the NRC public website at <http://www.nrc.gov>, under Electronic Reading Room/Document Collections.