U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH

DRAFT REGULATORY GUIDE

January 1996
Division 5
Task DG-5005

Contact: S.D. Frattali (301)415-6261

DRAFT REGULATORY GUIDE DG-5005
(Proposed Revision 1 to Regulatory Guide 5.15)

TAMPER-INDICATING SEALS FOR THE PROTECTION AND CONTROL OF SPECIAL NUCLEAR MATERIAL

A. INTRODUCTION

The Nuclear Regulatory Commission requires certain licensees to use tamper-indicating devices for material control and accounting (MC&A) and for physical security of special nuclear material (SNM). In 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," paragraph 70.51(e)(1)(i) requires that licensees authorized to possess and use SNM of moderate strategic significance or more than one effective kilogram of strategic special nuclear material (SSNM) in irradiated fuel reprocessing operations maintain, among other things, procedures for tamper-safing containers or vaults containing SNM not in a state of chemical or physical processing.

In 10 CFR Part 71, "Packaging and Transportation of Radioactive Material," paragraph 71.43(b) requires that "The outside of a package must incorporate a feature, such as a seal, which is not readily breakable, and which, while intact, would be evidence that the package has not been opened by unauthorized persons."

In 10 CFR Part 73, "Physical Protection of Plants and Materials," paragraph 73.26(g)(3) requires that SSNM be shipped in containers that are protected by tamper-indicating seals. Also, 10 CFR 73.46(c)(5)(ii) requires that certain SSNM be stored in tamper-indicating containers. Further, 10 CFR 73.46(d)(10) requires that, before exiting a material access area, containers of contaminated wastes

FOR COMMENT

This regulatory guide is being issued in draft form to involve the public in the early stages of the development of a regulatory position in this area. It has not received complete staff review and does not represent an official NRC staff position.

Public comments are being solicited on the draft guide (including any implementation schedule) and its associated regulatory analysis or value/impact statement. Comments should be accompanied by appropriate supporting data. Written comments may be submitted to the Rules Review and Directives Branch, DFIPS, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555. Copies of comments received may be examined at the NRC Public Document Room, 2120 L Street NW., Washington, DC. Comments will be most helpful if received by **April 12, 1996.**

Requests for single copies of draft guides (which may be reproduced) or for placement on an automatic distribution list for single copies of future guides in specific divisions should be made in writing to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Office of Administration, Distribution and Mail Services Section.

must be tamper-sealed by at least two individuals who do not have access to material processing and storage areas and who work and record their findings as a team.

In 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material," paragraph 74.59(f)(2)(i) requires that licensees authorized to possess and use formula quantities of SSNM develop procedures for tamper-safing containers or vaults containing SSNM not in process.

For safeguarding SNM of low strategic significance, the use of tamper-indicating seals is specifically required only during transit (see 10 CFR 73.67(g)(iii)). Nonetheless, licensees subject to 10 CFR 74.31 and 74.33 often find it convenient and economical to ensure long-term validity of MC&A measurements by tamper-safing the container in which the material is stored, thereby avoiding the expense of verifying the container's SNM content.

This guide is being developed to describe features of security seal systems and types of seals that are acceptable to the NRC staff for tamper-safing containers of SNM. Compliance with this guide is not required; existing systems or commitments in NRC-approved fundamental nuclear material control plans need not be modified to correspond with this regulatory guide.

Regulatory guides are issued to describe and make available to the public such information as methods acceptable to the NRC staff for implementing specific parts of the Commission's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and guidance to applicants. Regulatory guides are not substitutes for regulations, and compliance with regulatory guides is not required. Regulatory guides are issued in draft form for public comment to involve the public in the early stages of developing the regulatory positions. Draft regulatory guides have not received complete staff review and do not represent official NRC staff positions.

Any information collection activities mentioned in this regulatory guide are contained as requirements in 10 CFR Parts 70, 71, 73, or 74, which provide the regulatory bases for this guide. The information collection requirements in 10 CFR Parts 70, 71, 73, and 74 have been approved by the Office of Management and Budget, Approval Nos. 3150-0009, 3150-0008, 3150-0002, and 3150-0123, respectively.

B. DISCUSSION

In 10 CFR 74.4, tamper-safing is defined as "the use of devices on containers or vaults in a manner and at a time that ensures a clear indication of any violation of the integrity of previously made measurements of special nuclear material within the container or vault." Using this definition, a tamper-indicating seal is a device used to detect unauthorized removal of material.

Note that the phrase "container or vault" is used here in a broad sense. It includes all containers and secured storage enclosures for which the application of a tamper-indicating seal to the container or enclosure can be used to detect unauthorized access to the SNM within.

TAMPER-INDICATING SEALS

Various types of seals have been developed to meet specific requirements. Seals must be inspected to determine whether entry into the container or vault or tampering has occurred, as opposed to an active detection alarm that indicates when entry or tampering is occurring. Seals, when broken, are difficult to reassemble without leaving signs of tampering. Seals also have unique identification characteristics that show evidence of any attempt at forgery.

Different types of seals have essentially the same elements, but different properties. A key property of seals is frangibility, that is, they are easily broken. A seal is not expected to present a serious obstacle to entry or tampering, and for that reason it is usually a weak obstruction that can be overcome with small mechanical effort. In the past, the strategy was to make it very difficult for unauthorized persons to obtain seals from the manufacturer, in order to prevent cover-ups by replacing broken seals with new ones. With sophisticated modern seals, the unique identification characteristic (fingerprint) of the seal makes such replacements obvious.

FUNCTION OF A SEALING SYSTEM

A sealing system consists of (1) the seals themselves, (2) the procedures, techniques, and devices used in controlling seals, including procuring, documenting, storing, distributing, and, where appropriate, fingerprinting the

seals, as well as selecting the point of application, (3) applying, removing, and identifying the seals, and (4) judging whether entry or tampering has occurred.

The objective of a tamper-indicating sealing system is to provide assurance that no tampering or entry occurred while the seal was on the container. Therefore, for MC&A purposes, the measurements made before sealing, or for nondestructive analysis after sealing, are still valid. The degree of confidence in a tamper-indicating sealing system will vary directly with the effort required to defeat the seal and inversely with the motivation for defeating it. If a scheme for diversion of the contents requires undetected tampering with the sealed object, the seal presents an added obstacle that makes the diverter undertake extra activities. The chance that the diverter will make a mistake and be detected is therefore increased.

In order to use seals properly, the licensee needs to develop procedures that address (1) the control of access to tamper-indicating seals, (2) the unique identification of each seal, (3) records of the date, time, and person who applied each seal to a container or vault, and (4) other pertinent records of all such seals (this may include attesting documentation, see the appendix to this guide).

LIMITATIONS OF SEALING SYSTEMS

The most successful methods of attack on sealing systems are those exploiting the weaknesses of the sealing system rather than the tamper-indicating seal itself. A sealing system would fail at the seal if the seal could be opened and re-closed without leaving any marks to indicate tampering. Such a scenario would be difficult for the types of seals discussed in this guide.

A sealing system that depends on blank seals being unavailable to the adversary can fail if the supplier of the seals or one of his employees can be persuaded to provide replicates to a diverter. This type of failure presupposes a weakness in the identification of the seals. Therefore, all users of seals should require assurance from the manufacturer of the seals that the seals are unique, that the seals will not be supplied to other users, and that the masters will be controlled.

A sealing system can fail if the administrative controls are not adequate in the following areas.

- The information taken and recorded at the time of seal application is inadequately protected, enabling a diverter to forge documentation to support or cover the diversion.

- The selection of the application point for the sealing device does not provide assurance that it will indicate tampering.

- The method of postmortem examination of the seal is not sufficient to detect a defective or compromised seal.

- The location and method of seal application makes the seals vulnerable to accidental damage, providing a history of such incidents that might be used to conceal a willful attack.

- Inspection of the container's outer surface (or the walls or barriers of an enclosed storage area) is not sufficient to detect unauthorized access or penetration that bypassed the seal.

- The information being protected (such as SNM content), for SSNM or SNM of moderate strategic significance, is not attested to by at least two individuals at the time of seal application, or the information being protected for SNM of low strategic significance is not attested to by at least one individual at the time of seal application.

SEALS USED FOR SAFEGUARDING SNM

There are six commercially available seals that are sufficiently reliable for safeguarding SNM. These seals are the pressure-sensitive seal, the steel padlock seal, the type E cup-wire seal, the car/ball end seal, the active fiber optic seal, and the passive fiber optic seal.

Pressure-Sensitive Seal

Guidance on the testing, control, and application of pressure-sensitive seals for the onsite storage of SNM is provided in Regulatory Guide 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material."

Steel Padlock Seal

The steel padlock seal is a one-time seal that is destroyed when removed. The most secure design at present requires a hammer to drive a hardened steel shackle into a steel block. This seal is very rugged and may be used when accidental damage is likely and a lock is also needed. Unlike other tamper-indicating seals, this seal was designed to be used as a serious obstacle to entry.

Type E Cup-Wire Seal

The type E seal is a cup-wire seal in which a fingerprint may be artificially created by inscribing scratches on the inside surfaces of the seal; the scratches are photographed before the seal is applied. At the container inspection point, the seal is removed and sent to a laboratory for analysis and comparison with the original photograph. The seal is destroyed in the examination. The disadvantage in using this seal is the undesirable time lapse between removing the seal and getting the report back from the laboratory to the custodian who removed the seal.

The type E seal, when fingerprinted, is considered a high-security seal. That is, defeating the seal by forgery would require such an accurate reproduction of internal surface details that differences would not be distinguishable in a microphotographic comparison. Defeating the seal would require penetration and repair techniques that would not leave any visible evidence under a microscopic examination of the surfaces. While the seal could be defeated by cutting and rejoining the wire without leaving marks, the use of multi-strand wire makes undetectable rejoining extremely difficult.

Car/Ball End Seal

The car/ball end seals are steel strap seals. A latching mechanism, a piano-wire loop that captures both ends of the strap, is located inside a crimped ball at one end of the strap. The tip of the seal is designed to extend

through the lock housing and can be easily viewed through a special sight-inspection hole in the housing. The company's name, logo, and sequential serialized identifiers can be embossed on the seal strap.

Once the car/ball end seal is in place, it should be checked to ensure that there is a proper amount of end play in the latching mechanism. The seal is destroyed when it is removed for examination. The person conducting the postmortem examination should compare the removed seal to a sample seal and carefully inspect the exterior and interior surfaces to detect forgery. The ball housing should be opened to verify that all the internal parts are present. Compromise of the seal takes more than 5 minutes to perform and requires the use of special tools.

Fiber Optic Seal Systems

Fiber optic seal systems consist of fiber optic loop material, seal bodies, and a seal signature reader-verifier. Two types of fiber optic seal systems are commercially available, (1) active reusable and (2) passive single use. Active reusable systems are primarily used in the transportation of nuclear materials. The system is active in the sense that its electronic seal body sends an encoded digital pulse stream through the fiber optic loop to check for continuity. This design enables the detection and recording of the time, date, and duration of each fiber loop event, whenever the digital signal is interrupted. Opening the fiber loop or removing the fiber termination from the receptacle results in an "open" indication. An external housing around the seal body is necessary to prevent inadvertent opening of the loop. Seal-tampering information is obtained by attaching the seal to a reader and retrieving the stored contents of the seal. This reading is done in situ, without affecting the seal's integrity.

Passive single-use seal fiber optic systems are primarily used in long-term storage of nuclear materials. The fiber optic cable can be cut in the field to any length, up to 30 meters. The cable ends are inserted into a one-piece seal body. The seal body contains a serrated blade that, when pressed in place, severs a portion of the cable fibers in a random manner. This unique signature can be viewed and recorded by a seal reader at the loop termination. The seal is verified by comparing the image obtained during the inspection visit to the image obtained when the seal was initially installed.

C. REGULATORY POSITION

1. ACCEPTABLE SECURITY SEALS

The six types of security seals identified below are acceptable to the NRC staff for use in ensuring detection of unauthorized tampering or entry and in ensuring the accountability of SNM.

1.1 Pressure-sensitive seals as described in Regulatory Guide 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material."

1.2 Padlock seals, provided they are made of hardened steel that is capable of resisting cutting by a hacksaw. The shackle and the block should each carry a serialized identifier.

1.3 Type E seals, provided the crown-like clasping device is hot pressed or soldered to the top of the cylindrical cup. The wire passing through the hasp of the enclosure to be sealed should be a stainless steel cable with a minimum of 19 strands.

1.4 Car/ball end seals, provided the steel-strap seal is installed according to the manufacturer's instructions. The ball housing should be opened in the postmortem examination to verify integrity.

1.5 Active fiber optic seals, provided an external housing is installed around the body of the active seal to prevent unauthorized or inadvertent opening of the fiber loop. The fundamental nuclear material control plan should include a battery replacement schedule; batteries are not to be replaced when the seal is in use.

1.6 Passive fiber optic seal, provided the seal reader-verifier device provides clear images for inspection comparisons.

2. SEALING SYSTEM

A sealing system should include the following features to be acceptable to the NRC staff.

2.1 The outer surface of the seal should carry a serialized identifier and the name, logo, or initials of the organization using the seal. The lettering and numbering should be readable and should be engraved, molded, punched, or otherwise applied in a way that prevents removal or alteration of the letters and numbers without leaving apparent damages. The seals should be sequentially numbered with sufficient alphanumeric or numeric symbols to prevent duplication of symbols in use at the facility.

2.2 A seal should be applied to a container in a manner that ensures the contents cannot be removed from the sealed container without compromising the integrity of the seal or the container. A seal should be applied immediately after the samples and data have been taken to identify and measure the contents of the container. For nondestructive analysis measurements, the measurement may be taken after the seal is applied.

2.3 The design and construction of a seal should ensure that disassembly and reassembly of the seal would result in obvious indications of tampering that are detectable by the postmortem examination techniques recommended for the seal.

2.4 A seal should be resistant to, or be protected against, the effects of the environment or rough treatment that would be detrimental to the seal components and could give false indications or destroy any indications of tampering.

2.5 Seals should only be available to, applied by, and removed by persons designated by and responsible to MC&A management. The unused seals and the seal records should be maintained by a custodian in a secure location. Removed seals should be disposed of in a manner that prevents reuse.

2.6 Records of all seals, by serialized identification, should be retained after application. These records should include all pertinent data on the sealed contents, such as the container item number; location number or area; the dates, times, and reasons for application and removal of the seals; the signatures of the individuals responsible to MC&A management for the data and for applying and removing the seal, and a description of any discrepancy that is observed in the sealed contents.

2.7 Written procedures should be prepared that cover the control, application, documentation, postmortem examination, and reconciliation of seals. If the postmortem examination is made by a person other than the custodian removing the seal, procedures should be established to maintain the chain of custody of the removed seal.

2.8 Samples from every batch of seals received from the seal supplier should be retained for future reference and comparison in case of detected tampering. Samples should be maintained by a custodian and should be kept in a secure location.

APPENDIX

DECLARATIONS ON THE CHARACTERISTICS OF TAMPER-INDICATING SEALS

For each tamper-indicating seal that is applied, documentation should be provided that attests to all the following characteristics that are applicable.

1. Any identifiers such as numbers on the container, item, or seal numbers.

2. The type and form of the material within the container.

3. A statement that only the material stated in Number 2 above was placed in the container during loading.

4. A statement that nothing has been added or removed from the container since the loading or since breaking the previous seal.

5. The gross weight of the container, with units.

6. The net weight of the material, with units.

7. Upon replacement of a broken outer container seal, a statement that the integrity of the inner items remains intact.

8. A statement that material is not concealed or shielded within the equipment or container to avoid detection.

9. Whenever a container is resealed, a statement of the quantity of material added or removed from the container; zero quantities should be noted.

10. A statement on the status of the current vault or storage area contents relative to any change in the SNM inventory.

11. The quantity of the material as determined by nondestructive assay.

12. A statement that nothing has been added to or removed from the container during continuous surveillance.

DRAFT VALUE/IMPACT STATEMENT

1. PROPOSED ACTION

1.1 Description and Need

This guide provides guidance on features of security seal systems and it describes types of seals that are acceptable to the NRC staff for tamper-safing of special nuclear material (SNM). This guide was originally issued in January 1974. A revision to this guide is needed to bring it up to date with respect to current regulations and technology.

1.2 Value/Impact

1.2.1 NRC Operations

The regulatory position will be brought up to date.

1.2.2 Other Government Agencies

Not applicable.

1.2.3 Industry

Existing systems or commitments in NRC-approved fundamental nuclear material control plans need not be modified to correspond with this revision. Using the tamper-indicating systems discussed in this guide would have no adverse impact on the industry.

1.2.4 Public

No adverse impact on the public can be foreseen.

1.3 Decision on the Proposed Action

Revised guidance is needed to reflect the improvements in tamper-indicating technologies for the protection of SNM.

2. TECHNICAL APPROACH

Not applicable.

3. PROCEDURAL APPROACH

Revision of the existing regulatory guide is the appropriate way to make this information available to licensees.

4. STATUTORY CONSIDERATIONS

4.1 NRC Authority

Authority for the proposed action is derived from the Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974, as amended, and implemented through the Commission's regulations.

4.2 Need for NEPA Assessment

Revising this regulatory guide is not a major action that may significantly affect the quality of the human environment and does not require an environmental impact statement.

5. RELATIONSHIP TO OTHER EXISTING PROPOSED REGULATIONS OR POLICIES

Revising this regulatory guide is not directly related to any proposed regulations or policy. The proposed guidance is consistent with existing regulations.

6. SUMMARY AND CONCLUSIONS

The proposed guide should be issued for public comment.

Printed on recycled paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

FIRST CLASS MAIL
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67