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

August 2009
Division 5

DRAFT REGULATORY GUIDE

Contact: S. Ward
(301) 492-3426

DRAFT REGULATORY GUIDE DG-5029

(Proposed Revision to Regulatory Guides 5.10 and 5.15, dated July 1973 and March 1997, respectively)

PRESSURE-SENSITIVE AND TAMPER-INDICATING DEVICE SEALS FOR MATERIAL CONTROL AND ACCOUNTING USE

A. INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) requires its licensees to use tamper-indicating devices (TIDs) for material control and accounting (MC&A) and for physical security of special nuclear material (SNM). The requirements for the use of seals are contained in 10 CFR Part 71, "Packaging and Transportation of Radioactive Material" (Ref. 1); 10 CFR Part 73, "Physical Protection of Plants and Materials" (Ref. 2); and 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material" (Ref. 3).

This regulatory guide (RG) replaces the existing RG 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material," issued July 1973 (Ref. 4) and the existing RG 5.15, "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material," issued March 1997 (Ref. 5), with a new regulatory guide titled, "Pressure-Sensitive and Tamper-Indicating Device Seals for MC&A Use." As a replacement, this guide describes a number of improved TIDs and PS seals developed in recent years, primarily in response to commercial interests outside the nuclear industry. This guide, among other things, distinguishes between genuine and nongenuine manufactured seals and stresses serial number identification to aid in the control of commercial theft or to alert shipping and warehousing personnel to containers that were opened in transit. This guide also incorporates suggestions for ensuring that TIDs are properly applied.

The NRC issues regulatory guides to describe to the public methods that the staff considers acceptable for use in implementing specific parts of the agency's regulations, to explain techniques that the staff uses in evaluating specific problems or postulated accidents, and to provide guidance to

---

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 final staff review or approval and does not represent an official NRC final staff position.

Public comments are being solicited on this 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 Rulemaking and Directives Branch, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001; submitted through the NRC's interactive rulemaking Web page at http://www.nrc.gov; or faxed to (301) 492-3446. Copies of comments received may be examined at the NRC's Public Document Room, 11555 Rockville Pike, Rockville, MD. Comments will be most helpful if received by October 13, 2009.

Electronic copies of this draft regulatory guide are available through the NRC's interactive rulemaking Web page (see above); the NRC's public Web site under Draft Regulatory Guides in the Regulatory Guides document collection of the NRC's Electronic Reading Room at http://www.nrc.gov/reading-rm/doc-collections/; and the NRC's Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html, under Accession No. ML091670070.

applicants. Regulatory guides are not substitutes for regulations, and compliance with them is not required. This regulatory guide has no information collection requirements.

DISCUSSION

Background

The existing RG 5.15, "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material," issued March 1997, describes several types of commercially available TIDs, one of which includes PS seals for use in the MC&A of SNM. RG 5.15 considered, among other things, the function and limitations of these seals for various MC&A applications, particularly focusing on the protection of SNM in transit between facilities.

This revised RG replaces RG 5.15 as well as RG 5.10, which concerns only PS seals on containers used for onsite storage of SNM. This revised RG examines all MC&A-related uses, including PS seal devices that did not exist when RG 5.10 was originally written. In a U.S. Department of Energy report, issued December 1986 (Ref. 6), eight types of seals, including a "paper" seal (but not including fiber-optic seals), were evaluated to determine and compare the amount of time required to defeat each type of seal (i.e., breaking, removing, and reassembling the seal without leaving any signs of tampering). The report noted that, except for the paper seal, the time required for removing and replacing the original seal varied between 15 seconds and 60 minutes. The report also indicated that the paper seal was not defeated; however, the study provided no concrete evidence regarding the expertise of the person who attempted to defeat the seals.

Early PS seals were inexpensive compared to other types of TIDs. Seals available in 1986 were rudimentary compared to the technology of PS seals in use today. This is discussed in Section 2.4. In addition, past NRC findings show that TIDs, including PS seals, can and have been defeated when used incorrectly. The question remains as to how easily they can be defeated under the constraints imposed by the conditions of their application. This is discussed in Section 2.2.

1. NRC Requirements

1.1 Requirements in 10 CFR Part 71

In 10 CFR 71.43(b), the NRC requires that all package designs to be approved by the NRC incorporate a feature, such as a seal, on the outside of the package that is not readily breakable and that, while it is intact, would be evidence that unauthorized persons have not opened the package. The words "not readily breakable" are usually interpreted by NRC staff as referring to accidental breakage during routine handling.

1.2 Physical Protection Requirements in 10 CFR Part 73

In 10 CFR 73.26(g)(3), the NRC requires licensees to ship strategic special nuclear material (SSNM) in containers that are protected by tamper-indicating seals. In 10 CFR 73.46(c)(5)(ii), the NRC requires licensees to store certain quantities of SSNM in tamper-indicating containers, and in 10 CFR 73.46(d)(10), the NRC requires licensees to seal certain containers of contaminated waste before these containers are removed from a material access area to ensure that they are not used as a means for removing SSNM from the area.

1.3 Material Control and Accounting Requirements in 10 CFR Part 74.59

Those Category I licensees authorized to possess and use formula quantities of SSNM are subject to specific requirements defined in 10 CFR 74.59(f)(2)(i) and 10 CFR 74.55(a)(1), which require that licensees authorized to possess and use formula quantities of SSNM develop procedures for tamper-safing containers, for vaults containing SSNM that is not in active process, or for controlled access areas that provide protection at least equivalent to tamper-safing. SSNM that is in active use is subject to separate process monitoring requirements.

1.4 Material Control and Accounting Requirements in 10 CFR Part 74.43

Those Category II licensees who are authorized to possess and use SNM of moderate strategic significance are subject to the detailed requirements of 10 CFR 74.43(c)(3), which requires that licensees authorized to possess SNM develop, maintain, and follow procedures for tamper-safing containers and vaults containing SNM.

1.5 Material Control and Accounting Requirements in 10 CFR Parts 74.31 & 74.33

Those Category III licensees authorized to possess SNM of low strategic significance are subject to the detailed requirements of 10 CFR 74.31. In 10 CFR 74.33, the NRC defines similar requirements for uranium enrichment facilities. Although these requirements do not specifically refer to "tamper-safing," licensees must maintain a current knowledge of the items and store them in a manner such that they can detect unauthorized removal of substantial quantities. Category III licensees often find it convenient to use tamper-indicating seals to ensure the long-term validity of measurement data.

2. Seal Characteristics

2.1 Seal Functionality

NRC regulations require licensees to consider specific security procedures and to implement them to ensure that they achieve an acceptable level of protection of SNM at all times. The use of tamper-safing devices on containers or vaults is one such level of protection used to secure the integrity of SNM either when it is in transit or stored on site. The one overriding objective of TIDs is to ensure that no tampering or entry has occurred while the seal is on the container. Therefore, for MC&A purposes, the degree of confidence in the selection of a TID sealing system will vary depending on its unique characteristics and intended use. There are various types of commercial seals developed to meet specific NRC requirements. Although these seals have essentially the same elements, their properties are different. For example, a key property of seals is frangibility (i.e., they are easily broken). Because a seal is not expected to present a serious obstacle to entry or tampering, it is considered a weak obstruction that an unauthorized person can overcome with little effort. Thus, before procuring or using any TIDs, licensees should be certain that they clearly understand what they are trying to accomplish and should evaluate the use of available seals in terms of this understanding.

TID seals on containers used for onsite storage of SNM are passive devices that indicate, upon inspection, whether tampering or entry has occurred. TID seals may also identify where a theft may have occurred in the transportation chain. Receiving warehouses often do not open shipping cartons until the contents are needed. Therefore, the discovery of missing items raises the question, of whether the items were stolen in transit or in the warehouse.

In these cases, a TID seal would not need any serial identification or holographic logo but rather a clear and immediately indication that the carton had been opened. If an unauthorized person had tampered with the TID seal before the shipment arrived, it should be readily apparent that a theft most likely occurred in transit. Likewise, if the warehouse accepts shipments with seals intact and later finds a broken seal, a theft most likely occurred during storage.

Thus, the function of a tamper-indicating seal in the context of MC&A space is to ensure that a container or vault is properly closed and secured against accidental opening, authorized but undocumented opening, or unauthorized opening. If a TID seal has not been tampered with, the container has not been opened, and its contents are most likely still intact. If the TID seal has been tampered with, the container has most likely been opened, and assurance that the contents are intact is lost, even though nuclear material may or may not be missing. An accidental opening of a container (e.g., if an operator happens to open the wrong container) is the least likely scenario. Historically, authorized but undocumented openings most commonly occur when an operator is instructed to resample a container and then fails to document the changed net weight. The unauthorized opening of a container presumably is for the purpose of theft of all or a portion of the contents.

2.2 Pressure-Sensitive Seal Limitations

The most successful methods used to attack sealing systems are those that exploit the weaknesses of the sealing system rather than the tamper-indicating seal itself. A sealing system would fail at the seal if it could be opened and reclosed without leaving any marks that would indicate tampering. All tamper-indicating seals, including PS seals, can be defeated given adequate time and resources. In the context of MC&A space, the question is not whether unauthorized persons can defeat the seal, but whether they can defeat it given the available time and resources under the constraints imposed by the conditions of its use. For example, when a seal is used as part of a disarmament agreement that nuclear weapons will not be removed from long-term storage, it is necessary to recognize that the presumed adversary has time measured in months and essentially unlimited resources. When a seal is used in a high-security material access area, it is equally necessary to recognize that the presumed adversary has limitations on what tools or chemicals he or she can bring into the area and a time constraint that may be measured in minutes.

In the past, written reports (Refs. 7 & 8) differed in their conclusions regarding the correlation between the time required to defeat a seal and the cost of the seal itself. Licensees should consider the reported vulnerability of TIDs being defeated in the context of the situation in which the device is used. Those who have evaluated various seals for tamper resistance have generally limited themselves to what they termed “low-tech” approaches whereby the individual performing the tampering does not have any assistance from other individuals. On the other hand, the evaluations have allowed for the fabrication of a tool at a local machine shop or the purchase of chemicals from a chemical supply company to defeat the seals. The evaluations also presumably allowed the exchange of cooperative advice on how to develop a defeating technology. If, with practice, a person can learn a technique for defeating a PS seal that works half of the time but damages the seal half of the time so that tampering is obvious, the statement “the seal can be defeated” should be qualified to note that, with practice, the seal sometimes can be defeated but that there is also a significant risk of failing and leaving evidence of the attempt.

All TID seals are subject to the four potential vulnerabilities discussed below.

2.2.1 Substitution

All seals are vulnerable to being destructively removed and replaced by new seals. Under this scenario, the potential exists for an entire sealed container to be removed (e.g., stolen) and replaced with an identical container (i.e., one that is empty or that contains only low-value material) bearing a new seal.

In this situation, TID seals are of value only if the seals used are uniquely identified and this identity cannot be duplicated. Those individuals performing the unauthorized act should not have access to a supply of blank seals that are not clearly distinguishable from the originals. 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 they are unique, that they will not be supplied to other users, and that the masters will be controlled. Most vendors advertise that their seal designs are protected and that they will not sell the same design to a second customer. To protect themselves against a breach of this understanding, licensees should take the following precautions:

- All TID seals should bear a unique logo. Printed logos should be applied using a process that ensures deep ink penetration. Holographic logos, which are available from several suppliers, are harder to duplicate.

- Seals should be manufactured in a bright, easily recognized color. Some vendors consider red to be the default color, but the use of red is not essential if the color is also used for other purposes. Licensees can use color-coded seals to provide each seal custodian with a unique color, or the color-coded seals can denote the particular type of nuclear material (e.g., plutonium, mixed oxide, highly enriched uranium, or low-enriched uranium).

- All seals should bear a unique serial identification imprinted by the manufacturer. Unlimited possibilities exist, but the numbering sequence should provide enough numbers to last longer than the likely lifetime of the seal design. The serial numbers should be short and as simple as possible to help seal custodians quickly recognize whether the serial numbers are correct or not. One or two letters can be added to identify the material balance area so that each seal custodian can have a unique set of seals. The inclusion of more than one or two leading zeros (e.g., 0000012345) should be avoided. If the numbering sequence becomes exhausted, licensees should have the seals completely redesigned, even if technology improvements do not mandate the adoption of a new sealing system.

2.2.2 Removal and Reapplication

TID seals are vulnerable to being removed and reapplied. The NRC found cases where TID seals consisting of braided metal wires were improperly applied, leaving a significant amount of extra wire in the looped portion of the seal enabling the wire to be cut and replaced into the trap. Proper application of TID seals is essential to preventing this type of failure (e.g., pulling the excess wire all the way through the trap). PS seals are also subject to removal and reapplication. The NRC found cases where plastic seals were applied to surfaces where the seal had not been properly tested for leaving evidence of removal. Therefore, it is important that licensees consider the surfaces to which PS seals will be applied and the solvents that could be used to aid in removal of such seals. Before committing to a specific PS seal, licensees should develop a complete list of containers to which they will apply seals, and they should establish for each container those seals that cannot be removed and reapplied. Special cases relating to PS seals are presented hereinafter.

2.2.2.1 Removal Before the Adhesive Has Cured

Most adhesives develop full strength over a period of time, which can range from minutes to days. Many PS seals used in MC&A work are used only for a few days before the container is opened and the contents are processed. The licensee should establish the minimum-required curing time for PS seals with the vendor through testing. Procedures for using the seals should specify the length of time that sealed containers need to remain in the custody of the person(s) who applied the seal to allow for the adhesive to develop adequate strength.

2.2.2.2 Removal without Solvents

An unauthorized person should not be able to remove a PS seal by any means available. Most PS seals will not peel away when simply pulled at one edge, but many seals were developed for use on Kraft paper envelopes, corrugated cardboard cartons, or plywood boxes. Some adhesives that work well on those surfaces do not necessarily work as well on steel, stainless steel, glass, or plastic. Some PS seals may be removable from these latter surfaces with the careful use of a razor blade scraper.

Some adhesives lose their adhesive properties when they are subjected to climate change such as extreme cold. Placing a container in deep freeze for 1 hour is a viable scenario only if a suitable deep freezer is available. Also, the plastic seal itself undoubtedly will become very brittle when it is subjected to extreme cold, and any attempt to remove the seal may fracture it.

Even if the manufacturer states that the removal of a seal is not possible, the licensee should confirm this by testing seals to see if they can be removed from the containers on which they are to be used. The licensee should confirm the results by using the manufacturer's documented procedures and the samples used. The experiments should be documented, both with regard to what was tried and observations as to the degree of success in removing the seals. If, after 5–6 trials, the experimenter has not succeeded in lifting more than a small portion of the seals, the licensee can consider the seals acceptable. If the experiment achieved partial success in removing the seals and if the seals otherwise have desirable features, the licensee may wish to perform more extended testing. If, after multiple attempts, the experiment cannot extend occasional partial success into complete success, the licensee can accept the seal. If any significant number of attempts leads to complete success, the licensee should choose another seal or restrict the seal to containers for which success was not possible.

2.2.2.3 Removal with Solvents

It should not be possible to remove a seal by softening the adhesive with any solvent that is easily available within the facility. Kraft paper, corrugated cardboard, and plywood have porous surfaces. Any attempt to use solvents to remove a seal is likely to leave evidence of tampering. Metals, glass, and plastics have nonporous surfaces and are not likely to be affected by solvents (although some plastics may dissolve or swell when they come in contact with some solvents). The seal manufacturer may be able to advise licensees on what solvents will or will not work; if not, licensees should perform controlled testing. As a minimum, the licensee should test the following solvents:

a. water,
b. alcohol or ethylene glycol (antifreeze),
c. acetone or other easily available ketones,
d. naphthalene, toluene, or xylene (lacquer thinner or paint remover),
e. gasoline, kerosene, or mineral spirits,
f. quaternary ammonium solvents (some brand-name household cleansers), and
g. any solvent chemical that the licensee uses either as part of its nuclear operations or as a cleaning solvent.

Benzene, chloroform, carbon tetrachloride, and the trichloroethylene family of dry cleaning agents may be more difficult to obtain, but licensees should consider them as possible solvents for the removal and reapplication of seals. Specialized chemicals that can only be obtained from chemical supply houses are more questionable if they are not used in the facility and are therefore not readily available through that route. In addition to considering the availability of solvents, licensees should

consider whether existing security procedures would prevent the transport of a solvent into a nuclear material control area.

Industrial cleaners and the brand-name liquid cleansers that are available from supermarkets may work well in removing PS seals, but they may also destroy the adhesive or bleach the pigment. If they do not noticeably alter the seal itself, the licensee should consider whether the seal could be reapplied using commercially available glue.

If containers are intended for continual use or for cleaning and reuse, licensees should consider whether the procedures used for this cleaning and reuse would also facilitate the unauthorized removal and reapplication of the seals.

2.2.3 Alteration of Label Data

It should not be possible to alter recorded data on the TID or PS seal without the alteration being apparent. In past years, PS seals often served as container labels on which the operator wrote information, such as the batch number or net weight. With today's highly computerized systems, the serial identification number, which is permanently printed on the seal, may be the only recorded information. The computer then uses that number to correlate the container with separately recorded batch and measurement data. If the licensee must hand-record data on seals, it should establish that this information cannot be erased or washed off without the alteration being readily apparent.

Licensees should not rely solely on a serial number on a seal for container identification because removal or attempted removal of the seal will render the serial number unreadable. In this case, a facility may lose access to information about the contents of the container. Container numbers that are separately marked on containers will help licensees identify the container and its supposed contents even when the seal has been removed or destroyed.

2.2.4 Alteration of Separately Recorded Data

Licensees should control computerized or hand-written data associated with sealed containers to prevent or detect any attempt at unauthorized alteration of that data. Protection of recorded MC&A data is outside the scope of this RG, but it is still an essential part of using tamper-indicating seals. A seal might be defeated and the MC&A records altered to reflect the quantity left in the container. If neither falsification were detected, the theft would be discovered only as part of the inventory difference at the time of the next physical inventory. Another possibility is that the theft involves an unsealed quantity and that the MC&A records on sealed quantities are altered to conceal the theft. This theft will never be detected as long as the falsely described sealed container is left in storage.

2.3 Practical Considerations

One important practical consideration is how the seal is affixed to the container. Nearly all TIDs other than PS seals assume that the container has been constructed in such a manner as to facilitate the application of a seal. Other than the 200-liter (55-gallon) drum, many containers in common use in the nuclear industry are not constructed to facilitate the application of seals. Plastic bottles are used in a range of sizes and shapes; all have screw lids and no way to secure a seal. Ten-liter corrugated cardboard "ice cream cartons" are used for dry materials, especially scrap and waste. These containers have a snug-fitting slip on the lid but no provision for fitting a seal.

PS seals are ideal for these types of containers because they adhere well and cannot be removed. A screw lid cannot be removed without being unscrewed; any small seal that would break if the lid were

unscrewed should work well. Lids that simply slip onto containers may be more of a problem. If a corrugated cardboard carton can be deformed sufficiently to remove the lid without breaking the seal, then either two seals should be used, or the seal must cover more than one point. A strip seal that can be wrapped around the container-lid joint would probably work and would be preferable to a seal that crosses over the top to seal the container-lid joint at two opposite locations. In any case, the licensee should verify, for all containers for which seals are to be used, that the chosen seal will prevent the container from being opened.

Another practical consideration is the reuse of previously sealed containers. If a container is to be reused, then the licensee should remove the remnants of the previous seal by either scraping them off or by using solvents. The question of removal for undetected reapplication no longer applies, so razor blade scraping, which causes a PS seal to break into pieces, is acceptable. Also, removing a PS seal with industrial or household cleansers will destroy the seal in the process of cleaning. Most facilities prefer not to spend time removing remnants of past seals and would prefer to apply new ones. The licensee should verify that, for all containers intended for multiple uses, remnants of any previous seal can be removed with an acceptable amount of effort.

Some TIDs such as PS seals often are designed on the assumption that they will be applied to a flat surface. Extending a seal across the top of a container and down a portion of one side may introduce a bend, which the PS seal interprets as an attempt at tampering. Licensees should verify that seals will not self-destruct during application.

2.4 Commercially Available Tamper-Indicating Device Seals

There are several types of commercially available seals comprising a very broad range of capabilities. This guide describes some commercially available seals that are acceptable to the NRC for safeguarding SNM. Other seals may be approved on a case-by-case basis.

2.4.1 Steel Padlock Seal

The steel padlock seal is a one-time seal that is destroyed when removed. The most secure design 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 TID seals, this seal was designed to be used as a serious obstacle to entry.

2.4.2 Type E Cup-Wire Seal

The Type E seal consists of two metallic cups and wire. The ends of a loop of wire are passed through the hasp (one of the cups) and crimped together. The two cups are then pushed together, enclosing the crimped ends of the wire.

A fingerprint of the seal 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 Type E seal, when finger-printed, is considered a high-security seal. 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 difficult.

2.4.3 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 easily be 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.

2.4.4 Fiber Optic Seal System

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 optic 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 seals integrity.

Passive single-use seal fiber optic systems are primarily used in long-term storage of SNM. 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.

2.4.5 Tamper-Evident Wire Seal

The tamper-evident wire seal consists of a braided metal wire that has one end permanently attached to a solid metal trap. The other end of the braided metal wire is then loped through the container of SNM and is then inserted through a hole in the solid metal trap that is designed such that once the wire is inserted through the trap, it can not be pulled back through or otherwise removed unless the wire is cut. These seals use stranded-non-braided or loosely-braided metal wire that is designed to fray when cut (i.e., the individual strands separate due to the release of tension) making it extremely difficult to re-insert all of the strands back into the trap.

2.4.6 Pressure-Sensitive Seal

Based on work reported in the literature (Ref. 8), there are at least 25–30 commercially available PS seals. Many of these seals have a number of features in common. In selecting PS seals, licensees should consider the need for additional equipment (e.g., how many laser pens will be needed if a laser-encoded seal is selected), the need for operator training, the extent of the documentation that will be needed, and the time and effort needed for seal verification.

All vendors advertise that they recognize the importance of protecting seal designs and thus will not sell the same design to any second purchaser. Most vendors also advertise that they will destroy all production scrap, including any excess production not delivered to the purchaser. Licensees should explore this question explicitly with all prospective vendors to ensure a clear understanding that the seal design that the vendor is prepared to offer is protected.

The licensee should also consider the possibility that a seal could accidentally break. The effort that is required to investigate one accidentally broken seal could easily far exceed the added cost of seals that are less susceptible to accidental breakage.

2.4.6.1 Security Decals

The simplest PS seals are those referred to as security decals or void tapes. A security decal consists of a piece of vinyl, which may be virtually any size or shape, bearing whatever printed information is desired. (Most security decals are, strictly speaking, not decals.) A serial number can be included, and this serial number can be a barcode form for ease of verification or inventory. Most security decals are designed to peel easily even from paper; however, when they are peeled away from a surface, they leave the word "void" (or whatever word is chosen) on that surface. Security decals are inexpensive, and the ease of removal makes them suitable for containers intended for repeated use. It is questionable whether they provide sufficient security for use with SSNM or for offsite shipments. Some Category II or Category III licensees may consider security decals adequate for internal use to preserve the integrity of measurement data.

2.4.6.2 Optically Variable Devices (Holograms)

The optically variable image, or hologram, is well established as a technology that is easy to use and verifiable in the field. Whether it can be counterfeited depends on how much effort one is willing to apply. Small-town job shop printers usually do not have the equipment and expertise to produce holographic images, but any large city shop can produce holograms. A holographic company logo should be considered for inclusion when PS seals are selected and designed, but they add little to tamper resistance.

2.4.6.3 Multiple-Layer Security Tapes

A PS seal of necessity consists of at least three layers. On top is the vinyl or other material used as the seal. Next is a layer of adhesive, and finally there is a removable slip-sheet layer that protects the adhesive until the seal is to be used. The addition of a second vinyl layer and a second layer of adhesive can make a seal considerably more difficult to remove nondestructively. The intermediate adhesive is considerably weaker than the adhesive holding the seal to the container, and simple attempts to peel the seal away from the container will separate the layers, leaving at least part of the design still on the container.

Multiple-layer security tapes applied to paper, cardboard, or wood provide considerable tamper resistance. By carefully using a razor blade scraper, a person can often remove a multiple-layer security tape applied to glass with the tape remaining sufficiently intact to pass a casual verification. Licensees who choose to use multiple-layer security tapes should test the seals on the containers on which they are to be used.

2.4.6.4 Tamper Tape Seals

The tamper tape seal was developed as a less expensive, yet reasonably secure, alternative to an ultrasonic intrinsic tag that Pacific Northwest Laboratory developed in anticipation of Strategic Arms Reduction Treaty applications (Ref. 9). The top layer consists of glass beads embedded in a brittle bonding material. If transfer is attempted, the beads are disrupted from the bonding layer, and the logo pattern reflected from beneath the glass beads is distorted. Verification of the logo pattern requires visual observation with a light source such as a small flashlight held perpendicular to the surface of the tamper tape seal.

The tamper tape seal can be removed by subjecting it to extreme cold, which causes the adhesive to lose its strength. Licensees who may want to use the tamper tape seal should consider whether extreme cold (at least -4 °Fahrenheit (-20 °Celsius)) is a factor under the conditions of use.

2.4.6.5 Optical Chemical Coatings

Optical chemical coatings are not in themselves seals. However, they are relevant because they can be incorporated into PS seals and because doing so gives the seals considerable additional tamper resistance. The coating is transparent when viewed directly. When viewed from different angles, the image contained in the coating (e.g., the company logo) changes from transparent (invisible) to orange and then to green. The coating is not itself a thin film but rather a chemical coating having no structural strength. It self-destructs if there is any attempt to remove the seal in which it is incorporated. Also, the coating cannot be duplicated by any currently available graphic technology.

2.4.6.6 Laser-Encoded Seals

Some manufacturers offer seals with optically coded information that can be viewed only with a special hand-held laser device. The information recorded could be a corporate logo or it could be the serial identification number. Unlike the microprinting used on U.S. currency, optically coded information cannot be read under high magnification, nor can it be copied or optically remastered. Because the subsurface image is not obvious either to the naked eye or under high magnification, this offers security advantages over holograms.

2.5 Seal Verification

The integrity of all types of seals needs to be verified at the time the seals are removed. Many seals need periodic verification while still in use. TID seals selected for MC&A use should be field verifiable. Nearly all TID seals are destroyed when the container is opened.

During the periodic verifications required by 10 CFR Part 74, plant personnel should be able to confirm not only that the seal is still intact but also that it is the same originally applied seal and that it has not been tampered with. This does not mean that seal integrity should necessarily be apparent “at a glance.” The tamper tape seal described in Section 2.4.6.4 above requires examination in the light of a flashlight shining perpendicular to the seal surface. Another type of seal requires examination through a lens. The seal with optically encoded information requires examination with a hand-held laser-viewing device. In all cases, however, the licensee can perform field verification and can make the decision based on field verification that the seal has not been tampered with.

3. Procedures for Using Tamper-Indicating Device Seals

3.1 Control of Seals before Use

At the time purchased seals are delivered, the manufacturer should provide the licensee with precise instructions. Accompanying paperwork should specify exactly how many seals are being delivered with beginning and ending inventory numbers, and receipt verification should be sufficiently clear to verify that all seals are accounted for. If seals are missing, the licensee does not necessarily need to discard the lot, but it should perform a detailed inventory to determine the missing serial numbers, and all individuals authorized to use the seals should be warned that the missing numbers will require immediate investigation if they appear later on containers.

Licensees should distribute seals only to individuals authorized to apply them or to custodians who will distribute them to users on an as-needed basis. Licensees should securely protect both distributed seals and the stock that is reserved for later distribution. There is no regulatory requirement to verify the inventory of unused seals at intervals, but this is generally good practice.

3.2 Seal Application

Only those individuals who are authorized and trained to apply TID seals to containers should apply them. Training should include instruction on the types of containers that can be effectively sealed with the available seals, the method used to apply seals, and verification that seals have been properly applied. In most cases, applying a seal to a container has no meaning unless the quantity of nuclear material in the container is known. Seal application procedures should include establishing that this is the case and that the measured quantity data are properly recorded.

Clear records need to be made regarding seal use. The minimum information that must be recorded includes the date of use, the identity of the person who applied the seal, the identity of the container to which the seal was applied, and the seal serial identification. If a serial number on the seal is used as a correlation with materials accounting data, then these accounting data must also be recorded.

In each building or material balance area, only one person should be the seal custodian and one or more other individuals should be authorized seal appliers. This limits the ability of either the custodian or the applier to falsify his or her own work. For SSNM subject to a two-man rule, the seal applier is subject to the same "second-person" constraint whether or not the seal applier is also the seal custodian. For SNM of less strategic importance where the two-man rule does not apply, the same considerations that led to a decision not to impose two-man restrictions on other activities should also lead to a decision not to require a separation between seal custodians and seal appliers. The important consideration is that proper procedures exist for the appropriate control and use of seals and that the necessary materials accounting data are properly recorded.

3.3 Seal Verification during Storage

The continued integrity of TID seals should be verified at intervals that will depend on the material under protection. Where feasible, containers should be stored in such a manner that the licensee can verify TID seals with a minimum of container handling. If containers are stored in protective overpacks or closed storage units, the licensee should consider applying the seals to the overpacks rather than to the containers.

Casual observation that every container appears to bear an intact seal does not constitute adequate seal verification. The verification should include an examination of the seal for evidence of tampering, an examination of the container itself for evidence of attempts to bypass the seal, and a determination that the seal has not been removed and replaced by comparing the serial number or other unique data recorded on the seal. For some seals, the person performing the verification may have to examine the seal under special lighting conditions or with a laser pen to read encoded information. If the person has a list of containers and applied seal numbers, he or she should be able to compare numbers on the containers with the list and to make appropriate checkmarks on the list. The alternative, which is slightly more time consuming, but better in terms of not allowing for careless work, is for the person performing the verification to record seal numbers as containers are verified and then to make an after-the-fact comparison with an inventory of what should have been present.

Information concerning the date and time of verification, the identity of the person doing the verification, and any noteworthy observations (e.g., "seal scratched, but integrity not compromised") should be recorded. Any pattern in the observations should be considered carefully. In the example given, the licensee may want to modify the conditions of storage to eliminate accidental scratching or other forms of damage that do not compromise seal integrity. If seals are still being scratched, the licensee may need to seek a more detailed explanation.

Under some conditions (e.g., receipt of sealed nuclear material from off site), a facility may need to verify seals that it did not apply and that do not match its own seal stock. The facility should ask the shipper to supply both a sample seal for visual comparisons and a list of serial numbers or other identifying data for the seals that are actually used. Including a list of serial numbers with shipping papers is common practice; making this information available to the individuals who should verify seal integrity is less common. Serial numbers in the MC&A department's files are of little value; a copy of those numbers should be made available to the individuals responsible for seal verification.

The reverse situation also arises. Under some conditions (e.g., shipment of sealed nuclear material to offsite locations), a facility may need to entrust seal verification to individuals in another location working for a different employer. The facility should supply the receiver not only with a list of serial identification numbers but also with a sample seal and with instructions for seal verification. With some seals (e.g., those using laser-encoded information), the receiver may need to obtain special equipment.

3.4 Seal Verification at the Time of Removal

When the contents of a sealed container are to be used, it is important that the facility perform one final seal verification procedure before the seal is removed. The seal should then be either removed and returned to the custodian or destroyed. While most often TID seals are destroyed upon removal, simple cancellations (e.g., writing "void" across the seal, tearing a PS seal in half and peeling off the two fragments, or discarding the TID seal in the nearest trash bin) are usually insufficient. If the seal can be removed even in a seriously damaged condition, it should be returned to the custodian who should either store it in the same manner as that of unused seals or completely destroy it. Section 2.2 above discussed "practicing" before attempting to defeat a seal; removed but incompletely destroyed seals constitute an easily accessible source of practice seals.

The facility should document the details of the final verification to the same degree as it would the details of seal application and interim verification. The facility should also record the date and time of seal verification and removal, the condition of the seal before removal, the identity of the individual(s) removing the seal, the disposition of the seal or seal fragments, and the disposition of container contents.

There should also be a notation to the effect that the individual(s) removing the seal compared the seal with the data recorded at the time that it was applied to the container and found no discrepancies.

3.5 Written Procedures

As with all other aspects of material control and physical security, it is important that licensees prepare written procedures, that they keep them current, and that they make them available to the individuals who actually do the work. Licensees should include the following topics in their written procedures:

- procedures for deciding who should be designated as seal custodians or seal appliers and for documenting the decisions made,
- procedures for the control of TID seals before they are used,
- procedures for applying TID seals to containers, including the types of containers authorized for use with TID seals, the method used to apply the seals and to verify that they are properly affixed, and the data that must be recorded at the time that the seal is applied to the container,
- procedures for both interim verifications and verifications before the removal of TID seals, including the frequency of verification, examinations to be performed, and data to be recorded,
- procedures for the disposition of removed seals or seal fragments or for the destructive removal of seal fragments before releasing the container for reuse,
- procedures to follow in the event that seal breakage, replacement, or tampering is detected,
- procedures for handling the accidental breaking of a seal, and
- training procedures, including any required testing.

C. REGULATORY POSITION

Provided that the licensee has considered the vulnerabilities, conditions of use, and other considerations as described in this RG, and followed the recommended procedures in this RG, the NRC staff generally accepts TID seals for use in complying with the various requirements in 10 CFR 71.43, 10 CFR 73, 10 CFR 74.31, 10 CFR 74.33, 10 CFR 74.43, and 10 CFR 74.51 through 10 CFR 74.59. The NRC will also consider the adequacy of licensees' proposed seal procedures as compared to the discussion in this RG.

To be acceptable, a sealing system based on TID seals should include the following features:

a. The seal should bear a unique serial identity combined with unique information that identifies the licensed facility using the seal. Both the serial identity and the logo or other identifying information should be applied in a manner that makes undetected removal difficult. The licensee should explicitly establish with the manufacturer that it will not

sell identical or closely similar seals to any second individual, that it will adequately safeguard print masters, and that it will destroy all printing waste in a manner that would preclude salvage.

b. The seals should be applied in a manner that ensures that the contents cannot be removed from the sealed container without compromising the integrity of the seal or the container.

c. Measurements to determine container contents and the seal application should be coordinated in a manner that ensures that the contents could not be changed between the time when the measurements were made and the seal was applied.

d. For seals used for offsite shipments or for any use where the seal may be exposed to the elements, the seal chosen should be able to withstand such exposure without alteration in a manner that might be confused with tampering or that might destroy any indications of tampering.

e. Seals should only be available to and only be applied and removed by individuals authorized for that purpose. Written procedures should ensure that individuals authorized to handle seals are properly trained and that they maintain proper records of the seals used, verified, and removed.

f. Removed seals should be completely destroyed or should be protected by seal custodians using the same procedures as those for unused seals.

g. Written records of seal use should be maintained.

Compliance with this guide is not mandatory. Existing systems or commitments in NRC-approved MC&A and physical security plans need not be modified to correspond with the discussion in this guide.

D. IMPLEMENTATION

The purpose of this section is to provide information to applicants or licensees regarding the NRC's plans for using this draft regulatory guide. The NRC does not intend or approve any imposition or backfit in connection with its issuance.

The NRC has issued this draft guide to encourage public participation in its development. The NRC will consider all public comments received in development of the final guidance document. In some cases, applicants or licensees may propose an alternative or use a previously established acceptable alternative method for complying with specified portions of the NRC's regulations. Otherwise, the methods described in this guide will be used in evaluating compliance with the applicable regulations for license applications, license amendment applications, and amendment requests.

REGULATORY ANALYSIS

Statement of the Problem

The NRC published Regulatory Guide 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material," in July 1973, (Ref. 2) and revised Regulatory Guide 5.15, "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material," in March 1997, (Ref. 3) to provide general guidance for an acceptable program using TID and PS seals to assist in assuring that the diversion or theft of SNM from containers in temporary onsite storage has not occurred. The TID seals should assist in assuring the validity of previously made measurements and should give particular consideration to the composition, seal properties, method of affixing, seal control, and quality assurance.

With the recent changes in the threat environment since 9/11, the NRC recognizes the need for significant revision of these guides to address newer technology, equipment, and measurement control procedures affecting MC&A activities. Furthermore, recent changes to 10 CFR required revision of these guides to provide information concerning compliance with the rules as currently stated in 10 CFR.

Objective

The objective of this regulatory action is to provide a more useful and up-to-date version of the MC&A guidance for managing and controlling SNM activities using TID and PS seals that indicate upon inspection whether unauthorized tampering or entry has occurred. The original July 1973 regulatory guide and the revised 1997 regulatory guide also addressed the same concerns.

Alternative Approaches

The NRC staff considered the following alternative approaches:

- Do not revise Regulatory Guides 5.10 or 5.15
- Update Regulatory Guides 5.10 and 5.15 separately
- Update Regulatory Guide 5.10 but do not update Regulatory Guide 5.15
- Do not update Regulatory Guide 5.10 but update Regulatory Guide 5.15
- Update both Regulatory Guides 5.10 and 5.15 and reissue them as one regulatory guide.

Alternative 1: Do Not Revise Regulatory Guide 5.10 or 5.15

Under this alternative, the NRC would not revise either regulatory guide, and the original version of RG 5.10 and the 1997 version of RG 5.15 would continue to be available. This alternative is considered the baseline or "no action" alternative and, as such, involves no value/impact considerations.

Alternative 2: Update Regulatory Guide 5.10 and 5.15 Separately

Under this alternative, the NRC would revise Regulatory Guide 5.10 and Regulatory Guide 5.15 separately and independently of each other. Both guides would be updated to reflect post-9/11 security requirements and current regulations contained in 10 CFR. However, as PS seals represent one type of TID seal and RG 5.10 and RG 5.15 reference each other, much of the discussion concerning proper use of TIDs and PS seals would be repeated in each guide or available only in one of the RGs. This would require licensees to follow the guidance of two separate guides for implementing one program concerning the use of TID seals for the protection of SNM.

Alternative 3: Update Regulatory Guide 5.10 but Do Not Update Regulatory Guide 5.15

Under this alternative, The NRC would revise Regulatory Guide 5.10 but not Regulatory Guide 5.15. This would provide the benefits of updating RG 5.10 to reflect post-9/11 security requirements and current regulations contained in 10 CFR as well as current best practices performed in industry. It would not provide a current and up to date version of RG 5.15, which would leave some of the guidance concerning TIDs, of which PS seals represent one type, out of date.

Alternative 4: Do Not Update Regulatory Guide 5.10 but Update Regulatory Guide 5.15

Under this alternative, The NRC would revise Regulatory Guide 5.15 but not Regulatory Guide 5.10. This would provide the benefits of updating RG 5.15 to reflect post-9/11 security requirements and current regulations contained in 10 CFR as well as current best practices performed in industry. It would not provide a current and up to date version of RG 5.10, which would leave some of the guidance concerning PS seals out of date.

Alternative 5: Update Both Regulatory Guides 5.10 and 5.15 and Reissue Them as One Guide

Under this alternative, the NRC would revise both Regulatory Guide 5.10 and Regulatory Guide 5.15 and reissue them as a single guide covering all aspects of TID and PS seal use. The single revised guide would be updated to reflect post-9/11 security requirements and current regulations contained in 10 CFR. The single guide would reference TID and PS seals currently in general use, including improved seals that have been recently developed. This guide distinguishes between genuine and non-genuine manufactured seals and stresses serial identification to aid in the control of commercial theft or to alert shipping and warehousing personnel to containers that have been opened in transit.. This guide provides a single and concise reference for determining how TID and PS seals can be used for the protection of SNM.

Conclusion

Based on this regulatory analysis, the staff recommends that the NRC revise Regulatory Guide 5.10 and Regulatory Guide 5.15 and reissue them together as a single regulatory guide. This guide is not mandatory for licensees. The requirements for the use of seals are contained in 10 CFR Part 71, 10 CFR Part 73, and 10 CFR Part 74. The question of whether licensees are using the specific seals described in this RG has not been examined. If licensees are using these specific seals, the guide serves primarily to document current practice. If licensees are using older seal technologies, the guide offers them an opportunity to consider whether a change would improve regulatory performance and reduce costs. Therefore, the impact of this RG may be either negligible or favorable to licensees, but it is not expected to increase the costs of license compliance in any instance.

GLOSSARY

pressure-sensitive seals—Pressure-sensitive seals are usually strips of paper or plastic used to "seal" containers in such a way that opening the container would in some way alter the seal, making it clear that an unauthorized opening had occurred. Most pressure-sensitive seals in current use involve several layers of paper or plastic and are designed to reveal any attempt at removing the seal, including an unsuccessful attempt.

tamper-safing—Tamper-safing, as defined in 10 CFR 74.4, "Definitions," means "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." Expanding on that definition, a tamper-indicating device (TID) is a device that provides tamper-safing information. In principle, a TID does not need to be a seal, but most TIDs in fact are seals. The expression "to seal a container" is in more common usage than the more precise expression "to tamper-safe a container" or "to apply a TID to a container." In practical terms, all three expressions convey the same meaning.

vaults and containers—In 10 CFR 74.4, the definition of tamper-safing allows the use of tamper-safing devices on both containers and vaults. The distinction is one of size and mobility. Vaults usually are large (at least relative to containers) and massive and are constructed to withstand considerable physical attack. In contrast, most containers can be opened easily. Both containers and vaults have one element in common—whatever is contained inside the container or vault, it cannot be removed, escape, or accidentally fall out unless the container or vault is opened. If the vault or container is suitably protected against an undetected or unauthorized opening, then licensees can presume that the contents are secure.

REFERENCES[1]

1. 10 CFR Part 71, "Packaging and Transportation of Radioactive Material," U.S. Nuclear Regulatory Commission, Washington, DC.

2. 10 CFR Part 73, "Physical Protection of Plants and Materials," U.S. Nuclear Regulatory Commission, Washington, DC.

3. 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material," U.S. Nuclear Regulatory Commission, Washington, DC.

4. Regulatory Guide 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Material," U.S. Nuclear Regulatory Commission, Washington, DC, July 1973.

5. Regulatory Guide 5.15, "Tamper-Indicating Seals for the Protection and Control of Special Nuclear Material," Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, March 1997.

6. DOE/DP-0035, "Safeguards Seal Reference Manual," U.S. Department of Energy, Washington, DC, December 1986.[2]

7. R.G. Johnston and A.R.E. Garcia, "Physical Security and Tamper-Indicating Devices," *Proceedings of the American Society of Information Science Mid-Year 1997 Meeting, May 31–June 5, 1997*, pp. 43–46. This report was also published as Los Alamos National Laboratory report LA-UR-96-3827 (1996).

8. B.W. Wright and H.A. Undem, "Tamper Tape Seals," *Proceedings of the 35th Annual Meeting of the Institute of Nuclear Materials Management, July 17–20, 1994*, Institute of Nuclear Materials Waste, Northbrook, IL, 1994, pp. 1161–1166.

---

[1] Publicly available NRC published documents such as Regulations, Regulatory Guides, NUREGs, and Generic Letters listed herein are available electronically through the Electronic Reading room on the NRC's public Web site at: http://www.nrc.gov/reading-rm/doc-collections/. Copies are also available for inspection or copying for a fee from the NRC's Public Document Room (PDR) at 11555 Rockville Pike, Rockville, MD; the mailing address is USNRC PDR, Washington, DC 20555; telephone 301-415-4737 or (800) 397-4209; fax (301) 415-3548; and e-mail PDR.Resource@nrc.gov.

[2] Copies of the non-NRC documents included in these references may be obtained directly from the publishing organization.