Department of Energy
Washington, DC 20585

DOE Packaging Certification Program
Qualification/Accreditation of ARG-US RFID Tag as a TID Seal

July 30, 2012

Background

The Nuclear Regulatory Commission (NRC) requires licensees possessing special nuclear material (SNM) to comply with requirements in 10 CFR 71, 73 and 74. The NRC generally accepts tamper indicating (TID) seals for use in complying with the requirements in 10 CFR 71.43, 10 CFR 73, 10 CFR 74.31, 74.33, 74.43, and 10 CFR 74.51 through 74.59. The function of a TID seal in the context of Material Control and Accounting (MC&A) of special nuclear material in 10 CFR 74 is to ensure that a container or vault is properly closed and secured against accident opening, authorized but undocumented opening, or unauthorized opening.

NRC Regulatory Guide (RG) 5.80 "Pressure-Sensitive (PS) and Tamper-Indicating Device Seals for Material Control and Accounting (MC&A) of Special Nuclear Material," December 2010 describes a number of improved TIDs and PS seals developed in recent years, primarily in response to commercial interests outside the nuclear industry. The RG distinguishes between genuine and nongenuine manufactured seals and stresses serial number identification to aid in the control of material or to alert shipping and receiving personnel to containers that were opened in transit. The guide also incorporates recommendations for ensuring that TIDs are properly applied.

RG 5.80 discusses seal limitations and states "*The most successful methods used to attack sealing system 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 indications of tampering. All tamper-indicating seals, including PS seals, can be defeated given adequate time and resources. In the context of MC&A, the question is not whether unauthorized persons can defeat the seal, but whether they can defeat it given the available time and resource under the constraints imposed by the conditions of its use*."

All TID seals are subject to four potential vulnerabilities:

(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 materials) 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. 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. The licensee should take the following precautions: (a) All TID seals should bear a unique logo; (b) seals should be manufactured in a bright, easily recognized color; and (c) all seals should bear a unique serial identification code imprinted by the manufacturer.

(2) Removal and Reapplication
TID seals are vulnerable to being removed and reapplied. Clear installation instruction describing proper application and uses of TID seals should always be available.
(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. Licensees should not rely solely on a seal serial number for container identification because removal or attempted removal of the seal will render the serial number unreadable. In this case, the 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. Pairing of codes (one on the TID and one on the container) may be used to ensure that TIDs remain attached to the proper container.

(4) Alteration of Separately Recorded Data

Computerized or hand-written data associated with seals for containers should be controlled to prevent or detect any attempt at unauthorized alteration of that data.

ARG-US RFID tag

ARG-US radio frequency identification (RFID) tag is a battery-powered, active sensor and wireless communication device with automatic alarm capabilities. The tag has a universal form factor for attachment to regulatory-authority-approved transportation containers, as shown below:

The ARG-US RFID tag includes a suite of sensors for seal, shock, temperature, humidity, radiation, and battery strength. The tag also has a non-volatile memory that can record and store encrypted data. Upon installation to a container, the tag can communicate, as well as register events (with time stamps), such as the opening or excessive shock of the container either during routine operation or unauthorized intrusion. Furthermore, verification of presence, or detection of absence, of tags (and containers) can be assured via continuous polling by an interrogator (or reader) controlled by a computer and linked to secured database and web servers in a control center. The sensors have adjustable thresholds for high and low alert/alarm settings; the alerts/alarms are automatic and instantaneous; and the polling intervals are programmable depending on the threat level and security posture, thus providing the state of health (SoH) of the container at all times. The ARG-US RFID system has been thoroughly tested in actual operating environment since 2008 and documented in a series of reports and papers. (See http://rampac.energy.gov/RFID/RFID.htm)

Comparison of ARG-US RFID Tag Seal with a PS/TID Seal

Table 1 compares a PS/TID seal and the ARG-US RFID tag seal, with its seal functionality and limitations defined in RG 5.80. The PS/TID seal could be any of those mentioned in RG 5.80; however, it should be noted that the seal sensor in the ARG-US RFID tag is a thin force-sensitive

membrane switch which is compressed by a bolt (or a tab) affixing the RFID tag to a container. This is different from the PS seals mentioned in RG 5.80 that are usually applied by adhesives.

Table 1. NRC RG 5.80 for PS and TID Seals

	RG 5.80 for PS and TID Seals	ARG-US RFID Tag Seal
1	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.	Each ARG-US RFID tag has a complex and unique electronic identification assigned by the manufacturer. This identity can be verified at any time wirelessly by the authorized operator. Logo, serial number, and other applicable identifiers are clearly marked and/or engraved on the tag body. The tags, when activated, cannot be removed from the container without triggering a seal sensor alarm. Any tampering will result in the activity being recorded in the tag's non-volatile memory with a time stamp. All other requirements stipulated for the PS/ TID seas described in RG 5.80 are applicable and attainable for the ARG-US RFID tag seal.
2	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.	Owing to the seal sensor in the ARG-US RFID tag, the contents cannot be removed from a sealed container without triggering an alarm. Additionally, any tampering activity will result in a time-stamped record being generated in the tag's non-volatile memory for subsequent verification.
3	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.	These stipulations can be attained with ARG-US RFID tag seal in exactly the same manner as with PS/ TID seals of RG 5.80.
4	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.	The robust construction of the ARG-US RFID tag seal – front plastic cover, back metal plate, and rubber gasket in between – can withstand the elements without changes of appearance or degradation of performance. Possible confusion from weather exposure versus tampering is significantly less likely than with PS/TID seals of RG 5.80.
5	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.	The administration of ARG-US RFID tag seals, including inventory control and physical application of the tags, can be structured in the same manner as that for the PS/ TID seals of RG 5.80. Qualified administrators/ custodians/operators and approved procedures are the same key elements to success as with PS/ TID seals of RG 5.80.
6	Removed seals should be completely destroyed or should be protected by seal custodians using the same procedures as those for unused seals.	ARG-US RFID tag seals, because of its durability and relative high cost, are not usually destroyed after each use. Rather, they are re-initiated and re-logged for the next operation or campaign. When not in use, they are in protected custody just like PS/ TID seals of RG 5.80.
7	Written records of seal use should be maintained.	This requirement is applicable for, and attainable with, ARG-US RFID tag seals.