Rulemaking for Enhanced Security of Special Nuclear Material

RIN number: 3150-AJ41

NRC Docket ID: NRC-2014-0118

Regulatory Basis Document

January 2015

Table of Contents

REGULATORY BASIS FOR RULEMAKING TO
ENHANCED SECURITY OF SPECIAL NUCLEAR MATERIAL

1. Introduction and Background

The U.S. Nuclear Regulatory Commission (NRC) is initiating this rulemaking to revise a number of existing security-related regulations, including the portions of Title 10, "Energy," of the *Code of Federal Regulations* (10 CFR) Part 73, "Physical Protection of Plants and Materials," relating to physical protection of special nuclear material (SNM) at NRC-licensed facilities and in transit. The specific objectives of this rulemaking are to update SNM physical protection requirements to:

- make generically applicable security requirements similar to those imposed by security orders issued following the terrorist attacks of September 11, 2001;
- consider risk insights gained from new National Laboratory studies, implementation and oversight experience, and international guidance;
- improve consistency and clarity of those requirements; and
- use a risk-informed and performance-based structure.

These objectives are discussed in greater detail in Section 3, "Regulatory Problem."

In 2006, the Commission approved the staff's schedules and resources for the Enhanced Security at Fuel Cycle Facilities rulemaking effort (NRC, 2006a). Subsequently, the staff considered it appropriate, efficient, and effective to also evaluate SNM transportation security at the same time as it evaluated SNM protection at fixed sites.

In addition to fuel cycle facilities, the scope of this regulatory basis also includes physical protection of SNM at other facilities that possess and use SNM (e.g., non-power reactors, research and development facilities, and industrial facilities) and the physical protection of those materials in transit. Medical isotope production reactors (e.g., reactors used to produce Molybdenum-99) not subject to 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," would be included in the scope of this regulatory basis and the subsequent rulemaking effort.

The scope of this regulatory basis does not include the physical protection of SNM at nuclear power reactors, when that SNM is protected by the physical protection requirements of 10 CFR 73.55. SNM that is not protected by the physical protection requirements of 10 CFR 73.55, for example SNM stored outside the protected area, would be covered by this rulemaking. The nuclear power reactor security regulations were amended in 2009 to include requirements which were previously imposed by security orders. The staff believes that the robust physical protection at nuclear power reactors using low enriched uranium fuel, that is designed to protect against radiological sabotage, is sufficient to provide protection against SNM theft and diversion for SNM located within the nuclear power reactor protected area.

The scope of this regulatory basis does not include the physical protection of SNM stored in an independent spent fuel storage installation, a monitored retrievable storage installation, or a geologic repository operations area. NRC actions to update the physical protection requirements for these three classes of facilities would be covered by separate NRC rulemakings and thus are not within the scope of this regulatory basis. Additionally, this regulatory basis does not include spent fuel located at nuclear power reactors which is protected under 10 CFR 73.55.

The scope of this rulemaking does not include aspects of fuel cycle security orders, discussed below, that are being addressed by other rulemaking efforts. These security orders included requirements to assess and protect computer systems and digital networks. The NRC has adopted a phased approach for evaluating the need to regulate facilities with digital assets. In 2009, the NRC issued a new regulation (10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks") to provide a regulatory framework and approach for the protection of digital computer and communication systems and networks at nuclear power reactors. Protection of digital computer and communication systems and networks at fuel cycle facilities, non-power reactors (NRC, 2012b) and other facilities is being addressed separately from this rulemaking.

The fuel cycle security orders also included requirements to assess the potential for lethal exposures to members of the public from radiological material or chemicals subject to NRC regulations based on site-specific conditions and to protect those materials above certain exposure limits. In SRM-SECY-11-0108, "Regulation of Chemical Security" (NRC, 2012a), the Commission disapproved the staff's recommendation to proceed with rulemaking for increased chemical security at NRC-licensed facilities. Therefore, the aspects of the security orders related to chemical security are not within the scope of this regulatory basis.

The scope also does not include the security orders for spent fuel transport because a separate rulemaking was completed in 2013 to amend 10 CFR 73.37, "Requirements for Physical Protection of Irradiated Reactor Fuel in Transit."

This regulatory basis (1) explains why the existing regulations or policies need to be revised to address identified regulatory issues as discussed in Section 3, "Regulatory Problem"; (2) explains how a change in the regulations can resolve the issue and identifies a number of different approaches that could address the regulatory issue; (3) explains why alternatives to rulemaking cannot resolve the problem and addresses other options considered and why they were not pursued; (4) provides the scientific, policy, legal, or technical information that supports the decision to undertake rulemaking; (5) discusses backfit considerations, as appropriate; (6) discusses stakeholder interactions in developing the technical portion of the regulatory basis and stakeholder views, to the extent known; (7) explains how the recommended rulemaking will support the NRC's Strategic Plan goals; and (8) explains any limitations on the scope and quality of the regulatory basis, such as known uncertainties in the data or methods of analysis. The regulatory basis also presents plans to develop or revise guidance to support the rule and lists documents that have been cited or otherwise factored into the development of the regulatory basis. The regulatory basis does not include proposed regulatory text or a section-by-section analysis of current versus proposed regulations.

A draft version of this regulatory basis (NRC, 2014) was published in the *Federal Register* (79 FR 34641; June 18, 2014) requesting public comment. The public comment period was originally scheduled to close on August 4, 2014; but following stakeholder requests, the NRC extended the comment period until October 17, 2014 (79 FR 42474; July 22, 2014). The staff considered the comments and made changes to the draft document. A discussion of stakeholder comments and substantive changes that were made to the document are presented in Section 7, "Stakeholder Interactions." One significant change from the draft is the removal of discussions for the Security-Force Fatigue at Nuclear Facilities rulemaking effort. During the comment period, Category I fuel cycle facility licensees proposed an alternative to rulemaking. The NRC considers an industry initiative a feasible alternative to rulemaking and has decided to separate the regulatory basis activities for the Security-Force Fatigue at Nuclear Facilities rulemaking effort from this document to allow time to adequately explore alternatives to rulemaking.

2. Existing Regulatory Framework

This section presents the regulatory history and chronology of the existing regulatory framework (including existing regulations, regulatory guidance, policies, licensing practices, and oversight such as inspection and enforcement) for the physical protection of special nuclear material (SNM). It is important to understand the legislative underpinnings for SNM protection, the state of knowledge and the basic policies of the Atomic Energy Commission (AEC) (a predecessor to the NRC) and of the NRC that established the existing Category I, II, and III physical-protection approaches. The information presented in this section provides the background of the current protection and categorization scheme and provides information as to why the various changes and new information, presented in Section 3, "Regulatory Problem," necessitate changes to the existing regulatory framework.

2.1 Regulatory History

The fundamental need and concept of grading for safeguards[1] was clearly and firmly embedded in the Atomic Energy Act of 1954, as amended (AEA). Section 53 of the AEA states, in part, that "special nuclear material shall be distributed only on terms, as may be established by rule of the Commission, such that no user will be permitted to construct an atomic weapon …" and that "the Commission shall establish, by rule, minimum criteria for the issuance of specific or general licenses for the distribution of special nuclear material …" and "is authorized to establish classes of special nuclear material and to exempt certain classes or quantities of special nuclear material or kinds of uses or users not inimical to the common defense and security and would not constitute unreasonable risk to the health and safety of the public." In 1956, when 10 CFR Part 70, "Special Nuclear Material," was published in the *Federal Register* (21 FR 764; Feb. 3, 1956), the AEC decided that neither substantively revised regulations for material control and accounting (MC&A) nor any physical protection were necessary because the high intrinsic value of SNM (i.e., the great monetary and time costs to create SNM) supposedly would be an industry incentive for voluntary MC&A and physical protection measures. In 1966, as a result of the enactment of private-ownership legislation and a 1965 incident in which a large

[1] Safeguards in the context of this document refers to the combination of physical protection and material control and accounting.

amount of highly enriched uranium went unaccounted for at a licensed fuel facility, the AEC amended Part 70 to set forth certain new MC&A requirements. However, the AEC continued to rely on the high intrinsic value of the SNM, statutory penalties for diversion, and present health and safety and material accountability programs as the primary factors in assuring that licensees would provide appropriate physical protection of SNM. These new MC&A requirements were graded based on a 5,000-gram threshold of uranium-235, plutonium, and uranium-233 to exclude those licensed facilities which used small research quantities of SNM.

Category I Physical Protection

In 1967, the AEC developed a classified study on the strategic importance of SNM, which was the cornerstone for the existing Category I, II and III categorization approach that is commonly followed by the NRC and the International Atomic Energy Agency (IAEA) for grading physical protection requirements. The various protection thresholds have largely been viewed as classified fractions of the types and quantities of SNM that would have to be illicitly acquired to manufacture an improvised nuclear device (IND). This approach assumed that potential adversaries possessed a certain general level of technical skill, competence and resources. In 1969, the AEC approved a new Part 73 for physical protection for SNM in transit (34 FR 6277; April 9, 1969). This rule introduced the concept of an external radiation dose-rate threshold of 100 rem per hour at 3 feet. Using simple covert theft scenarios, the AEC then believed that an external radiation level of that magnitude would act as an effective deterrent to the unauthorized removal of radioactive material. This threshold was based largely on a draft 10 CFR Part 20, "Standards for Protection against Radiation," health and safety standard for defining very-high-radiation areas (that radiation level in Part 20 was later increased in 1978 to 500 rad per hour at one meter upon its codification in final form for §20.203(c)(6)). The 100 rem per hour level was then applied - as an exemption - to simple covert theft scenarios for cargo storage cages at airports. In addition, the 1969 rule included an exemption from the physical protection requirements during transport for uranium enriched to less than 20 percent in the U-235 isotope. In 1970, the first physical protection regulation for fixed sites "use and storage" was published (35 FR 6313; April 18, 1970) and adopted the same exemptions as the preceding rules for in-transit SNM and included certain fencing, guards/watchmen, and patrol requirements.

The need for protecting domestic nuclear materials and facilities against a terrorist threat gained urgency following the terrorist attacks against Israeli athletes during the 1972 Munich Olympics. In 1973, the AEC published two comprehensive final rules that contained extensive revisions on theft of SNM and industrial sabotage of SNM in transit and at fixed sites (38 FR 30533 and 30537, respectively; November 6, 1973). These rules established a vast number of protection system concepts, features, and components that are required by the existing regulations. For example, this rule set forth the following requirements for fixed sites: (a) protective barriers and intrusion-detection devices to provide early detection of an attack, (b) deterrence to attack by means of armed guards and escorts, and (c) liaison and communication with law enforcement authorities capable of rendering assistance to counter such attacks. Extensive improvements for protecting SNM shipments in transit were also included. The rule added 10 CFR 73.50, "Requirements for Physical Protection of Licensed Activities" (which applied to nuclear power reactors and facilities with Category I material), and 10 CFR 73.60, "Additional Requirements for the Physical Protection of Special Nuclear Material at Fixed Sites" (which applied only to

facilities with Category I material). The physical protection measures included the requirement for two physical barriers (protected and vital area barriers) and specified the SNM formula for performing the Category I threshold computations.

In 1979, the last major amendment to SNM protection (i.e., the "Physical Protection Upgrade Rule") overhauled physical protection requirements for formula quantities of strategic SNM, which was designated as Category I SNM (44 FR 68184; November 28, 1979). At that time, licensees no longer held large amounts of separated plutonium because of the termination of plutonium recycling in the United States after President Carter's decision not to pursue spent fuel reprocessing. The Physical Protection Upgrade Proposed Rule introduced the concepts of the general performance objectives that a physical protection system was to provide: (1) "high assurance" that activities involving SNM are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety, and (2) performance capabilities for fixed-site and transportation physical protection (42 FR 34310; July 5, 1977). Furthermore, the rule consolidated design-basis threat[2] (DBT) requirements (previously for protecting nuclear power reactors against industrial sabotage) from the general performance objectives section of §73.55(a) to a new §73.1(a), where it was modified and became a radiological-sabotage DBT that was applicable to both nuclear power reactors and Category I SNM activities. The DBT threat description that was in §73.20(a) was also consolidated in §73.1, and a new §73.1(b) was created to specify a theft or diversion DBT that was only applicable to Category I SNM activities.

Radiological sabotage was discussed in the Upgrade Rule's Statement of Considerations. The Commission recognized that "although specifically designed to prevent theft, the new safeguards requirements would also provide increase protection against sabotage" (42 FR 34310; July 5, 1977). Later in the revised proposed rule, the staff retained the previous fixed-facility requirements in §73.50 (at the time, the nuclear power reactor and base Category I physical protection requirements) to make those older requirements applicable to Category I material that was irradiated and to spent fuel storage at locations other than nuclear power reactor facilities (43 FR 35321; August 9, 1978). To add clarity to protection requirements for spent nuclear fuel and high-level waste, a new regulation (10 CFR 73.51, "Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-Level Radioactive Waste") was issued in 1998 (63 FR 26955; May 15, 1998). Furthermore, that rulemaking excluded facilities subject to §73.51 from the requirements in §73.50.

Non-Power Reactors

As part of the Physical Protection Upgrade Rule, the Commission also stated,

> "Non-power reactors are not required to meet the provisions of the upgrade rule. As an interim measure, non-power reactors must meet the provisions of 10 CFR 73.67(a), (b), (c), [and] (d), (requirements for protection of material of low and moderate strategic

---

[2] A design-basis threat is a profile of the type, composition, and capabilities of an adversary. DBTs are used as a basis for designing safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material.

significance), and in some cases the provisions of a revised §73.60 (for those non-power reactor facilities possessing formula quantities of SNM not meeting the 100 rem per hour exemption). Application of the requirements of these amendments to non-power reactors possessing formula quantities of SNM which cannot meet the 100 rem per hour exemption was deferred pending completion of a separate on-going review of total safeguards requirements adequacy at such facilities. This is an interim solution only, and it is the intent of the Commission to bring non-power reactors under an improved safeguards system in the near future." (44 FR 68184; November 28, 1979)

A later revised proposed rule for non-power reactors stated that the 100-rem-per-hour exemption level might be difficult to maintain and could encourage unnecessary reactor operations just to meet that level. It proposed that "if a licensee can show that, for the theft of a formula quantity, it is reasonable to expect that a thief would receive an absorbed dose of at least 2000 rem, and then the licensee will only have to satisfy Category III physical requirements." The 2000-rem dose would be incapacitating within a short period and would mean certain death. This staff recommendation was not approved by the Commission (48 FR 34056; July 27, 1983). In 1993, 10 CFR 73.60(f) was added to the regulations to manage potential sabotage risk for non-power reactors with a power output greater than two megawatts (thermal) (58 FR 13700; March 15, 1993).

Category II and III Physical Protection

At the same time that the Upgrade Rule was issued, a separate Category II and III Rule (i.e., "Safeguards Requirements for Special Nuclear Material of Moderate and Low Strategic Significance") was issued to cover requirements for strategic SNM below the Category I threshold, low-enriched uranium, and irradiated SNM (44 FR 43280; July 24, 1979). Together, these two rules established the current NRC grading of classes of SNM physical protection requirements using a three-tiered categorization approach. The resulting SNM I, II and III Categories were consistent with recommended levels in IAEA's INFCIRC/225, Rev. 1, "The Physical Protection of Nuclear Material," (IAEA, 1975).

As discussed in the Category II and III Rule, the justification for Categories II and III were predicated on the following basis:

a. Protection of plutonium, uranium-233, and high enriched uranium[3] (HEU) can be justified on the grounds that a formula quantity (Category I) could be obtained through multiple thefts of Category II and III materials.

b. Protection of uranium enriched to less than 20 percent (low-enriched uranium (LEU)) might have technical justification based on the chance that without safeguards, it might be possible to divert such material out of the United States for additional enrichment or for production of plutonium without detection.

---

[3] High enriched uranium (HEU) is uranium enriched to at least 20 percent uranium-235.

c. Although nuclear materials may be involved in a threat to the public through a dispersion scenario, such as by sabotage, SECY-77-79, "NRC and International Physical Protection Standards," (NRC, 1977) states that the risk from dispersion of small or moderate quantities of nuclear materials (including irradiated materials) did not appear to pose a risk to the public sufficient to justify specific protection measures at that time.

Technical Underpinnings

The underlying rationale of the regulations discussed above was that protective measures should be commensurate with the potential consequences of malevolent acts to the public's health and safety or to the common defense and security. Such malevolent acts included both theft or diversion, and radiological sabotage. Grading of physical protection gave priority to SNM directly usable in an IND while making safeguards largely proportional to the ease of converting the SNM into a weapons-usable form. Risk-oriented grading associated with these rulemakings primarily provided the greatest protection to SNM which, if stolen or diverted, could be used to fabricate an IND.

The dominant strategy of the NRC, Department of Energy (DOE), and IAEA is to prioritize protective measures proportional to the ease of converting various kinds and forms of SNM to weapon-usable form. A cornerstone of the NRC's grading system is the concept of making an appropriate distinction between SNM that is directly usable in an IND as compared to SNM that is indirectly usable. Direct-use means the SNM does not need further enrichment or other major chemical or metallurgical processing steps before fabrication into an IND. In that sense, strategic SNM is direct-use material if it does not need substantial additional work to convert it into a better form for constructing an IND. Certain isotopic quality and material form attributes make particular SNM compositions and configurations indirect-use material (e.g., LEU and spent fuel).

NRC policy at the time of the last major revisions to the SNM physical protection regulations assumed that sub-national adversaries would lack sufficient means (i.e., process equipment, detailed knowledge and funding) to chemically or metallurgically process indirectly usable SNM (e.g., LEU or plutonium or uranium-233 in spent nuclear fuel (SNF)) into a form directly usable for the construction of an IND. Accordingly, past rulemakings assumed that any clandestine uranium enrichment and reprocessing of spent nuclear fuel operations were beyond the capabilities of terrorists operating in the United States (NRC, 1978a; NRC, 1982; NRC, 1984).

Adversaries acquiring LEU would have to perform additional steps to further enrich the material at a clandestine facility. Additionally, plutonium or uranium-233 in highly radioactive commercial SNF (which typically has high burnup levels) would have to be recovered (i.e., separated from other radioactive fission products in the SNF) in a clandestine hot-reprocessing plant. Optimally, it would be converted into a form for direct usage in an IND. Such adversary enrichment or hot-reprocessing capabilities have not been viewed as credible for a sub-national group (NRC, 1982).

Since President Carter's decision to terminate spent nuclear fuel reprocessing and plutonium recycling in 1978, virtually no separated plutonium has been licensed by the NRC. Very small amounts of uranium-233, totaling only hundreds of grams, are possessed and licensed in the

private sector. As a result, the preponderance of attention over the past 25 years shifted to safeguarding uranium-235.

2.2 Existing Regulatory Requirements

The existing SNM physical protection regulatory requirements at fixed sites and in transit are graded using a material categorization approach. The existing material categorization approach places uranium and plutonium in one of three risk-informed categories: Category I (i.e., formula quantity of strategic SNM), Category II (i.e., SNM of moderate strategic significance), or Category III (i.e., SNM of low strategic significance), depending on its type, quantity (i.e., mass), and enrichment for uranium-235. Strategic SNM consists of HEU, uranium-233, and plutonium. The regulations in Part 73 then identify requirements for physical protection of that SNM depending on its Category. The ease of separability of SNM from other radioactive materials and external radiation levels is also considered to a varying degree in assigning different physical protection requirements or in exempting certain materials from physical protection requirements. However, the regulations contain exemptions and exceptions under which material is not required to be protected within the three-category approach.
The regulations in 10 CFR 73.6, "Exemptions for Certain Quantities and Kinds of Special Nuclear Material," exempt licensees from the Category I protection requirements at fixed sites (i.e., 10 CFR 73.20, "General Performance Objective and Requirements"; 10 CFR 73.45, "Performance Capabilities for Fixed Site Protection Systems"; and 10 CFR 73.46, "Fixed Site Physical Protection Systems, Subsystems, Components, and Procedures") and in transit (i.e., 10 CFR 73.20; 10 CFR 73.25, "Performance Capabilities for Physical Protection of Strategic Special Nuclear Material in Transit"; and 10 CFR 73.26, "Transportation Physical Protection Systems, Subsystems, Components, and Procedures"). In addition, § 73.6 exempts other SNM materials from records and notification requirements (i.e., 10 CFR 73.70, "Records," and 10 CFR 73.72, "Requirement for Advance Notice of Shipment of Formula Quantities of Strategic Special Nuclear Material, Special Nuclear Material of Moderate Strategic Significance, or Irradiated Reactor Fuel") for the following materials:

(a) Uranium-235 contained in uranium enriched to less than 20 percent in the uranium-235 isotope;

(b) special nuclear material which is not readily separable from other radioactive material and which has a total external radiation level in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding;

(b) special nuclear material in a quantity not exceeding 350 grams of uranium-235, uranium-233, plutonium, or a combination thereof, possessed in any analytical, research, quality control, metallurgical, or electronic laboratory;

(c) special nuclear material that is being transported by the U.S. Department of Energy transport system; and

(d) special nuclear material at non-power reactors.

The regulations in §73.67(b) exempt a licensee from the requirements of 10 CFR 73.67, "Licensee Fixed Site and In-Transit Requirements for the Physical Protection of Special Nuclear Material of Moderate and Low Strategic Significance" for use and transport for (1) SNM which is not readily separable from other radioactive material and which has a total external radiation level in excess of 100 rem per hour at a distance of 3 feet from any accessible surface without intervening shielding, (2) sealed plutonium-beryllium sources totaling 500 grams, or (3) plutonium with an isotopic concentration exceeding 80 percent plutonium-238. Also, the regulations in §73.67(d) and (f) exempt Part 50 licensees from the requirements in these sections.

In addition, although small quantities of SNM may be licensed by Agreement States (10 CFR 150.10, "Persons Exempt," and 10 CFR 150.11, "Critical Mass"), persons in Agreement States who possess, use, or transport Category III SNM are required to meet the requirements of §73.67 (see 10 CFR 150.14, "Commission Regulatory Authority for Physical Protection").

SNM at Fixed Sites

Performance objectives of the physical protection systems for fixed sites are described in §73.20(a) for Category I material and §73.67(a) for Category II and Category III material. The performance objective for the physical protection of Category I materials is to provide high assurance that activities involving SNM are not inimical to the common defense and security and do not constitute unreasonable risk to the public health and safety. Physical protection systems for Category I material are designed to protect against the DBTs of theft or diversion and radiological sabotage. The objective of the physical protection system for Category II and III materials is to minimize the possibility for unauthorized removal of SNM and to facilitate location and recovery of missing SNM. The NRC's policy is not to require the physical protection systems of facilities with Category II and III materials and non-power reactors to protect against the DBTs of theft or diversion and radiological sabotage. Rather, for these facilities, the NRC's policy is to require licensees to meet a set of requirements, the effectiveness of which have been evaluated based on NRC threat assessments as well as consequence and security assessments for these facilities. For sites with Category I material, the existing regulations in §73.45 further specify that performance capabilities of a fixed site's physical protection system must meet the general performance requirements of §73.20(a).

Specific protection requirements are addressed in sections §73.46 (Category I material) and §73.67 (Category II and Category III material). The physical protection requirements are generally graded based on the risk of the material being used for malevolent purposes, with physical protection requirements for facilities with Category I material being more robust than those at facilities with Category II material, which are more robust than those at facilities with Category III material. For example, §73.46 specifies requirements for facilities with Category I material pertaining to (1) security organization, including training and qualifications; (2) physical barrier subsystems for protected areas, material access areas, and vital areas; (3) access-control subsystems for protected areas, material access areas, and vital areas; (4) detection, surveillance, and alarm subsystems, including multiple alarm stations; (5) communication subsystems; (6) testing and maintenance programs; and (7) contingency and response plans. In contrast, the requirements in §73.67(f) for facilities with Category III materials address access controls, response by a watchman or offsite response force, and

response procedures. In addition, access-authorization requirements are described in Part 11, "Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material," for Category I material and are described in 10 CFR 73.57, "Requirements for Criminal History Records Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility, a Non-Power Reactor, or Access to Safeguards Information," for non-power reactors. Access-authorization provisions are not specified in the existing regulations for Category II and III materials. The regulations do not have provisions to provide high assurance that individuals having access to other than Category I SNM and non-power reactors are trustworthy and reliable to use these materials as intended or will not aid or abet those with malevolent intentions.

Separate regulations are provided for protection of Category I SNM that is exempt from the requirements in §73.20, §73.45 and §73.46 under §73.6(b) and §73.6(e). The regulations in §73.50 specify physical protection requirements for Category I material that is not covered by §73.51; is not readily separable; and exceeds the external radiation dose-rate threshold. This regulation specifies requirements pertaining to (1) security organization, (2) physical barriers for protected areas, material access areas, and vital areas, (3) access control, (4) detection aids, (5) communication, (6) testing and maintenance, and (7) response. The requirements are generally less stringent than those specified in §73.46 for Category I material at other facilities.

Similarly, the regulations in §73.60 specify physical protection requirements for non-power reactors. The regulations state that Category I quantities of SNM at non-power reactors should be protected against theft or diversion under §73.67(a) through (d) (i.e., Category II protection requirements) in addition to the requirements in §73.60. However, Category I material at non-power reactors that is not readily separable and exceeds the external radiation dose-rate threshold is exempt from those additional requirements in §73.60. The additional requirements include access requirements, exit requirements, detection aid requirements, testing and maintenance requirements, and response requirements which are generally less stringent than those specified in §73.46 for Category I material at other facilities. In addition, §73.60(f) states that the Commission may require alternate or additional measures to protect against sabotage for non-power reactors above 2 megawatts (thermal).

Regulatory guides (RGs) provide guidance to licensees and applicants on acceptable methods for carrying out specific parts of the NRC's regulations, techniques used by the staff in evaluating specific problems or postulated accidents, and data needed by the staff in its review of applications for permits or licenses. RG 5.61, "Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites" (NRC, 1980b), was issued to help licensees in preparing security plans in response to the 1979 regulatory requirements. The principal RGs used in licensing Category I, II and III facilities are RG 5.52, "Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material at Fixed Sites" (NRC, 1994); RG 5.55, "Standard Format and Content for Safeguards Contingency Plans" (NRC, 1978b); and RG 5.59, "Standard Format and Content of a Licensee Physical Protection Plan for Special Nuclear Material of Moderate or Low Strategic Significance" (NRC, 1983). Other RGs address specific security topics at fixed sites (see http://www.nrc.gov/reading-rm/doc-collections/reg-guides/protection/rg/). In addition, the following NUREG documents provide guidance to licensees and applicants:

- NUREG-1322, “Acceptance Criteria for the Evaluation of Category I Fuel Cycle Facility Physical Security Plans” (NRC, 1991)

- NUREG-1456, “An Alternative Format for Category I Fuel Cycle Facility Physical Protection Plans” (NRC, 1992)

- NUREG/CR-6667, “Standard Review Plan for Safeguards Contingency Response Plans for Category I Fuel Facilities” (NRC, 2000b)

- NUREG/CR-6668, “Standard Review Plan for Training and Qualifications Plans for Security Personnel at Category I Fuel Facilities” (NRC, 2000c)

Category I, II and III licensees are inspected consistent with Inspection Manual Chapter (IMC) 2600, “Fuel Cycle Facility Operational Safety and Safeguards Inspection Program” (NRC, 2010), and other IMCs in the 2600 series. These provide guidance for assessing facility performance using the Licensee Performance Review process and in preparing for the annual Agency Action Review Meeting. Non-power reactor licensees are inspected in ways consistent with IMC 2545, “Research and Test Reactor Inspection Program” (NRC, 2004b). Inspection findings are dispositioned consistent with the NRC’s Enforcement Policy.

SNM in Transit

Performance objectives of the physical protection systems in transit are described in §73.20(a) for Category I material and §73.67(a) for Category II and Category III materials. In ways similar to the regulations for Category I material at fixed sites, the existing regulations in §73.25 further specify that performance capabilities of in-transit physical protection systems must meet the general performance requirements of §73.20(a). Physical protection requirements for SNM in transit are addressed in sections §73.26 for Category I transport, §73.67(e) for Category II transport, and §73.67(g) for Category III transport. In ways similar to the fixed facility physical protection requirements, physical protection requirements for material in transit are graded based on risk, with physical protection requirements for Category I transport being more robust than those for Category III transport. For example, §73.26 specifies requirements for the transport of Category I material pertaining to (1) planning and scheduling, (2) export/import shipments, (3) security organization, (4) contingency and response plans and procedures, (5) transfer and storage of strategic special nuclear material for domestic shipments, (6) access-control subsystems and procedures, (7) test and maintenance programs, (8) shipment by road, (9) shipment by air, (10) shipment by rail, and (11) shipment by sea. The physical protection requirements in §73.67(g) for the transport of Category III material address advance notifications and confirmation of shipments, tamper-indicating devices, response procedures, and import/export notifications. Also, 10 CFR 73.24, “Prohibitions,” requires NRC preapproval of shipment schedules for Category II transport. Notification requirements for Category I material are addressed in 10 CFR 73.27, “Notifications requirements”; while notifications are not required for Category II or Category III materials. 10 CFR 73.28, “Security background checks for secure transfer of nuclear materials,” excepts licensees from the security background-check provisions in Section 170I of the AEA if they have not received orders from the NRC containing requirements for background checks for trustworthiness and reliability that

include fingerprinting and criminal-history record checks as a prerequisite for unescorted access to radioactive materials.

As a matter of mutual understanding with the NRC, the Department of Energy's Office of Secure Transportation currently carries out the transportation and transportation security for Category I materials. For such shipments, the NRC has determined that Category I licensees are not required to have a transportation security plan for shipment of Category I material. The Office of Secure Transportation also carries out the transportation and transportation security for fresh and irradiated non-power reactor fuel and has committed to transporting fresh mixed-oxide fuel assemblies.

The principal RGs used in licensing SNM physical protection during transport are RG 5.60, "Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material in Transit" (NRC, 1980a), and RG 5.56, "Standard Format and Content of Safeguards Contingency Plans for Transportation" (NRC, 1978c). Other RGs address specific security topics during transportation.

10 CFR Part 74

Material Control and Accounting (MC&A) requirements are provided in 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material." MC&A and Physical Protection are part of the same discipline usually collectively referred to as safeguards. Safeguards are generally understood to be (1) measures taken to deter, prevent or respond to the unauthorized possession or use of significant quantities of SNM through theft or diversion and (2) measures taken to protect against radiological sabotage of nuclear activities. Typically, MC&A licensee programs, in accordance with Part 74, provide control and accounting measures to detect abrupt and protracted theft or diversions of SNM from authorized locations and processes within a facility. Physical protection licensee programs, in accordance with Part 73, consist of a variety of measures to protect nuclear facilities and material against sabotage, malicious acts, and theft or diversions that result in the removal of licensed material from the facility. MC&A requirements work together with a licensee's physical protection programs developed in accordance with Part 73, to create an integrated and complementary safeguards approach that results in a more robust protection against sabotage, theft, and diversion of licensed materials. The requirements within 10 CFR 74 are a graded approach based upon the category of special nuclear material.

10 CFR Part 11

Access-authorization requirements for Category I SNM are provided in 10 CFR Part 11, "Criteria and Procedures for Determining Eligibility for Access to or Control over Special Nuclear Material." This regulation includes requirements for SNM access authorization and criteria for determining eligibility for access to or control over SNM. The background checks include fingerprinting and criminal-history checks.

10 CFR Part 26

Fitness for duty program requirements are provided in 10 CFR Part 26, “Fitness for Duty Programs.” Fitness for duty programs help ensure that individuals are not under the influence of any substance or mentally or physically impaired from any cause that could adversely affect their abilities to safely and competently perform their duties and include drug and alcohol testing, behavioral observation, fatigue management, and employee assistance programs. Part 26 applies, in part, to holders of licenses for power reactors licensed pursuant to Part 50, “Domestic Licensing of Production and Utilization Facilities,” and 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.” Part 26, except for subparts I (Managing Fatigue) and K (Fitness for Duty Programs for Construction), also applies to Category I licensees under Part 70, “Domestic Licensing of Special Nuclear Material,” and certificate of compliance holders under 10 CFR Part 76, “Certification of Gaseous Diffusion Plants.”

3. Regulatory Problem

This section discusses issues with the existing regulatory framework and is organized in a way that follows the objectives of the rulemaking described in Section 1, “Background.” This section discusses the reasons that the existing special nuclear material (SNM) physical protection regulations are in need of enhancement or need to be changed. New information and technical studies that form the basis revising the existing regulations are discussed. The issues discussed below include 1) generic applicability of various security orders that have been issued by the NRC, 2) acquired risk insights related to a wide range of issues that involve physical protection, 3) lack of consistency and clarity in the existing regulations, and 4) use of a more performance-based and risk-informed regulatory approach.

3.1 Generic Applicability of Security Orders

The first objective of this rulemaking is to make generically applicable those physical protection requirements imposed on fuel cycle facilities by the security orders and on non-power reactors by confirmatory action letters. Changes to the threat environment highlighted by the terrorist attacks of September 11, 2001, caused the NRC to reevaluate its security programs. Understanding the DBTs and changes that were made to the DBTs is an important context for understanding why the security orders were issued and the basis for further changes to the existing regulations. To be consistent with separate DBT Orders issued in 2001 and as required by the Energy Policy Act of 2005, the NRC revised the attributes and characteristics of the DBTs for theft or diversion and for radiological sabotage to account for changes in the threat environment (72 FR 12705; March 19, 2007). Changes to the DBT considered several factors, including the events of September 11, 2001; an assessment of physical, cyber, biochemical, and other terrorist threats; the potential for attack on facilities by multiple coordinated teams consisting of a large number of individuals; the potential for assistance in an attack by several persons employed at the facility; the potential for suicide attacks; and the potential use of explosive devices of considerable size and other modern weaponry. The DBTs are based on realistic assessments of the tactics, techniques, and procedures used by international and domestic terrorist groups and organizations. The DBTs are developed by working with national experts and are based on classified and other sensitive information. The NRC also relies on the U.S. Intelligence Community, law-enforcement agencies, and State and local governments to

provide accurate and timely information about the capabilities and activities of adversary groups (NRC, 2013a). The NRC continuously evaluates threat-related information and makes changes to the attributes and characteristics of the DBTs as necessary.

In the aftermath of the September 11, 2001, terrorist attacks, the Commission determined that licensees should implement new security requirements to address the new threat environment. The Commission further determined that these requirements should be implemented through orders as opposed to a rulemaking to expedite licensee implementation of the requirements. Subsequently, the NRC performed evaluations and determined that additional physical protection measures were not required beyond those issued in the security orders to address the new threat environment. In SRM-COMSECY-05-0058, "Schedules and Resources for Security Rulemakings," (NRC, 2006a), the Commission directed the staff to incorporate the physical protection requirements contained in the security orders into regulations to make those requirements generically applicable, increase regulatory predictability and stability, and allow interested stakeholders to provide comments on these new security requirements as part of the rulemaking process.

Although the NRC did not issue security orders for SNM transportation (beyond those for transportation of spent nuclear fuel), on several occasions the NRC worked with licensee organizations to ensure that transportation security plans for specific shipments included security measures that were more stringent than those required in the existing regulations. Licensees enhanced their transportation security measures voluntarily. For example, the security measures for the shipment of a Category II quantity of HEU from the General Atomics facility in San Diego, CA to the Idaho National Laboratory in Idaho in 2010 were more robust than the requirements for Category II SNM shipments in §73.67(e). While this approach can be effective in specific cases, it has significant drawbacks, including inconsistency of security measures, lack of regulatory stability, lack of transparency to stakeholders, and significant resource implications for both licensees and the NRC.

Interim Compensatory Measures and Additional Security Measures Orders

In 2002 and 2003, the NRC issued orders for Interim Compensatory Measures to Category I fuel cycle facilities and for Additional Security Measures (ASMs) to Category III fuel cycle facilities to increase the physical protection at these facilities (Virgilio, 2002; Virgilio, 2003). Similar security orders were issued to new licensees. The NRC did not issue security orders to fuel cycle facilities with Category II material because the NRC did not and does not have a licensee that is considered a Category II SNM facility.

The security orders contain measures that were controlled as Safeguards Information or classified national security information; and therefore, those measures are not discussed in detail in this regulatory basis. In general, the changes in physical protection measures resulting from the security orders included enhancements such as the following: increased security patrols; augmented security forces and capabilities; additional security posts; additional physical barriers, including vehicle barriers; additional intrusion-detection capability; vehicle searches at greater standoff distances; additional random and mandatory personnel and package searches; evaluation and protection of computer and digital assets; enhanced coordination with local law enforcement and other governmental agencies; augmented security and emergency response

training, equipment, and communication, including consideration of offsite medical and emergency response capabilities and actions to be taken for an imminent threat; and more restrictive site access controls for personnel.

In 2002 and 2003, the staff transmitted letters to non-power reactor licensees recommending implementation of Additional Security Measures which focused on the mitigation of potential radiological sabotage and theft events. Most non-power reactor licensees voluntarily committed to carrying out at least some of these ASMs. Individual site implementation of various ASMs was inspected and confirmed through the issuance of confirmatory action letters. To be consistent with Section 104.c of the Atomic Energy Act and with Commission policy on utilization and production facilities that conduct research and development activities (namely, to impose only the minimum amount of regulation on these licensees necessary to promote the common defense and security and protect the public health and safety), the Commission issued confirmatory action letters rather than issuing security orders. The confirmatory action letters contain measures that were controlled as Safeguards Information; therefore, those measures are not discussed in detail in this regulatory basis. In general, the changes in physical protection measures resulting from the confirmatory action letters included enhancements such as vehicle barriers, background checks, coordination and communication with local law enforcement, vehicle and personnel searches, and visitor escorting.

Access Authorization Orders

Section 652 of the Energy Policy Act of 2005 (EPAct), enacted on August 8, 2005, amended the fingerprinting requirements of the Atomic Energy Act of 1954 (AEA). Specifically, the EPAct amended Section 149 of the AEA to require fingerprinting and a Federal Bureau of Investigation identification and criminal history records check for "any individual who is permitted unescorted access to utilization facilities, and radioactive materials or other property subject to regulation by the Commission that the Commission determines to be of such significance to the public health and safety or the common defense and security as to warrant fingerprinting and background checks." The Commission made such a determination for access to SNM, and between 2005 and 2007, the NRC issued orders to require fingerprinting and criminal history checks and determination of trustworthiness and reliability for unescorted access to material at fuel cycle facilities and non-power reactors. The trustworthiness and reliability determination was based on several factors including criminal history, verification of education and employment history, and personnel references; and later became the licensee's access authorization program. Fuel cycle facilities with Category III material were only required to carry out access-authorization requirements if they had areas resulting in significant chemical consequences (note that such requirements are beyond the scope of this regulatory basis, as discussed in Section 1, "Background"). Therefore, fuel cycle facilities with Category III material (for activities and consequences within the scope of this regulatory basis) were determined by the Commission not to require access-authorization requirements. The increased access-authorization requirements are in part intended to manage the risk of insiders conducting malevolent acts or colluding with adversaries. The NRC has made generally applicable similar requirements for access authorization programs in §73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants,", for fingerprinting and criminal history checks in §73.57, "Requirements for criminal history records checks of individuals granted unescorted access to a nuclear power facility, a non-power reactor, or access to Safeguards Information," and for radioactive material in Subpart B, "Background Investigations and Access Control Program," of 10 CFR Part 37,

"Physical Protection of Byproduct material." As part of the associated rulemakings, the staff developed a technical basis document for fingerprinting and authorization for unescorted access to radioactive materials which include SNM licensees (NRC, 2008). The staff considered this technical basis document when developing its proposed access authorization approach discussed in Section 4, "Basis for Requested Changes."

3.2 Risk Insights

The second objective of this rulemaking is to consider risk insights, and implementation and oversight experience in evaluating the need for regulatory change. Since the last major revisions to the SNM physical protection requirements in 1979 (discussed in Section 2.1, "Regulatory History"), significant changes in the regulated material and facilities have occurred. For example, the NRC currently regulates gas centrifuge enrichment facilities, and has licensed a mixed-oxide fuel (containing both uranium and plutonium) fabrication facility and a laser enrichment facility. The NRC has also received applications for medical isotope production facilities which will use SNM. Also, the policy restriction on reprocessing established by President Carter has been revised by subsequent administrations, and the NRC, as directed by the Commission in SRM-SECY-13-0093, "Reprocessing Regulatory Framework – Status and Next Steps," is expending limited effort towards resolving the regulatory gap associated with safety and risk assessment methodologies for a reprocessing-specific rule (NRC, 2013b). Moreover, future new reactor designs and associated fuels have the potential to change the mix of SNM beyond that historically licensed by the NRC.

In addition, following the events of September 11, 2001, the NRC and other governmental agencies undertook many studies (discussed below) to evaluate the risk and consequences associated with the physical protection of SNM and security at fuel cycle facilities and non-power reactors. These studies have identified new vulnerabilities and risks that were not considered in 1979 or in the existing regulations. The combination of the changes in types of facilities and materials being regulated by the NRC and risk insights from these studies led the NRC to question the current categorization approach and consider the benefits of using a more risk-informed material attractiveness approach for SNM in the grading of physical protection requirements for fixed sites and transportation. This new approach would better define physical protection requirements for SNM based on the attractiveness of the material for its use in an improvised nuclear device (IND). Considering material attractiveness in the determination of appropriate physical protection requirements will enable the "rightsizing" of physical protection regulations that are specific to quantities of various forms and concentrations of SNM. Moreover, this approach would establish physical protection requirements at fixed sites and for transportation based on the risk that the material could be used for malicious purposes, regardless of the facility, and therefore will reduce some of the inconsistencies discussed above. These studies also led the NRC to question the appropriateness of the current external radiation dose-rate threshold and the level of protection afforded by the current regulations to address greater sabotage risks.

The staff further considered the need for new physical protection requirements to manage certain risks and scenarios that were not addressed by security orders or existing regulations. Risk insights from other NRC regulatory programs are also considered, including consideration of synergies with material control and accounting (MC&A) programs. The staff recognizes that MC&A and physical protection programs share certain risk considerations, such as the relevant

internal adversary aspects in the DBT and comparable SNM thresholds for triggering protective measures against theft or diversion. The categorization approach postulated in this effort, which considers material attractiveness, could also be used by MC&A programs. Therefore, interactions between MC&A measures and physical protection measures can complement each other in managing the risk associated with the malevolent use of SNM. This positive synergy should be taken into account as part of this rulemaking when considering revisions to physical protection requirements. For example, the proposed requirement for an insider risk assessment for facilities with Category I material benefits both physical protection and MC&A goals. The staff also considered the need for new physical protection requirements based on implementation and oversight experience.

In addition, the IAEA recently revised its international standards pertaining to physical protection of nuclear material and nuclear facilities (i.e., International Atomic Energy Act, INFCIRC/225, Revision 5 (IAEA, 2011). This rulemaking considers alignment and consistency issues with international standards and guidance, and risk insights. These aspects are discussed in detail below.

Material Categorization and Attractiveness

One of the major components of this rulemaking is to risk-inform physical protection requirements against theft or diversion of SNM using a graded approach that considers material attractiveness. Material categorization and attractiveness inform the potential consequences of theft/diversion or loss of SNM and permit risk-informed approaches to formulating SNM physical protection requirements for fixed sites and transportation.

The current approach discussed in Section 2, “Existing Regulatory Framework,” does not consider certain aspects of the attractiveness of nuclear materials and could, in some cases, lead to SNM physical protection that is not commensurate with the risk significance associated with SNM of a particular type and form (i.e., the physical protection may, in some cases, be overly conservative). The NRC’s current approach defines an SNM category based on the quantity and type of material, and, in the case of uranium, its isotopic composition. The underlying assumption of this approach (discussed in Section 2.1, “Regulatory History”) is that an SNM category defines the associated security risk because it directly relates to the usability of nuclear material for IND construction.

In some situations and configurations, Category I amounts of SNM might not necessarily have high strategic significance. For example, 5 kilograms of high-enriched uranium (HEU) in metal form presents a greater risk than 5 total kilograms of HEU dispersed in a 120-ton gondola railcar filled with SNM-contaminated waste. Likewise, Category III SNM may not always be of low strategic significance in practice. Some of the chemical and physical forms of SNM represent less risk than others, even though the materials, despite their different chemical and physical forms, might fall into the same category. The existing regulations make no distinction based on material attractiveness and impose the same physical protection measures on both non-dilute and more attractive, and very dilute and less attractive, forms of SNM. For materials of low attractiveness, the regulations may be overly conservative and may require licensees to carry out physical protection measures far in excess of what is necessary to adequately protect SNM.

In addition, non-dilute forms of Category I quantities of plutonium require the highest level of physical protection. However, a fresh mixed-oxide (MOX) fuel assembly containing a Category I quantity of plutonium might not require the same physical protection measures as non-dilute plutonium because an adversary would have greater difficulty stealing a bulky and heavy item weighing several hundred kilograms. The adversary would also have to take extra chemical and mechanical processing steps to extract the plutonium from a MOX assembly. The NRC believes that diluted SNM offers an additional level of protection, and that alternative physical protection measures to detect theft and rapidly recover the missing material should still provide adequate security assurances.

As a result, the NRC has issued exemptions in license conditions to relax the physical protection measures based on the attractiveness of the SNM for use for malicious purposes or in an IND. Examples of these exemptions include the following:

- A licensee was exempted from Category I SNM physical protection requirements regarding the transportation of HEU-contaminated waste containing a Category I quantity of HEU; the licensee was allowed to transport the material with physical protection less stringent than that normally required for Category I SNM.

- A licensee was exempted from Category I SNM physical protection requirements regarding the storage and disposition of HEU-contaminated waste containing a Category I quantity of HEU; the licensee carried out a set of alternative security measures.

In these cases, the NRC determined that the level of protection allowed by the exemptions was appropriate because the SNM was dilute and not attractive to adversaries. The use of exemptions, while appropriate in these circumstances, has significant drawbacks, including the inconsistency of physical protection measures, lack of regulatory predictability, and significant resource implications for both licensees and the NRC.

Since the late 1970s, the NRC's understanding of the technical and security aspects of SNM theft scenarios has improved. The IAEA established a material categorization table, which is used to grade physical protection of SNM, in INFCIRC/225, Rev 1 (IAEA, 1975). This material categorization table is generally accepted internationally and, as discussed in Section 2.1, "Regulatory History," was used by NRC in developing its SNM physical protection requirements. Since the mid-2000s, the Department of Energy (DOE) considered the merits of changing the material categorization table to account for material attractiveness (DOE, 2000). In 2007, the DOE documented their assessment in "Technical Review of the DOE Graded Safeguards Table" (DOE, 2007). The assessment was based on studies, most of which are classified, that address technical aspects of IND construction, specific security scenarios of concerns, issues related to material categorization and attractiveness, and evaluation of SNM physical protection strategies and measures.

Following the DOE effort, the NRC carried out a comprehensive review of NRC regulations and assessed past and current approaches to security licensing and inspections at SNM facilities. The results of this assessment were presented in SECY-09-0123, "Material Categorization and Future Fuel Cycle Facility Security-Related Rulemaking" (NRC, 2009). Some of the key findings include: (1) the existing NRC approach is not consistent with the approach used by DOE; (2) implementation of physical protection measures at NRC-regulated facilities is not always

consistent; and (3) physical protection requirements might need to be adjusted for facilities of certain types (e.g., future reprocessing facilities). The NRC's review of past regulatory practices and the DOE work led the staff to assess the current regulatory approach to SNM categorization and attractiveness for NRC licensees.

As part of this assessment, the NRC contracted with Los Alamos National Laboratory (LANL) to carry out a technical study that would provide an updated assessment of SNM acquisition pathways and technical aspects of IND construction by potential adversaries. The LANL study considered adversary characteristics and capabilities that are consistent with changes to the DBTs. The staff notes that the assumptions related to adversary characteristics and capabilities and to the scenarios discussed in Section 2.1, "Regulatory History." have evolved; therefore, adversary characteristics and capabilities, and scenarios considered in the LANL study, might vary from the information in Section 2.1, "Regulatory History."

The LANL study and other recent reports have significantly advanced the staff's understanding of technical approaches that adversaries can take to process stolen SNM into a form suitable for use in an IND and to complete IND construction. The studies suggest that while many relevant chemical, metallurgical and fabrication processes have not changed in the past few decades, the availability of the associated technical knowledge and equipment has increased. With adequate time and resources, a potential adversary could be expected to chemically process SNM into a form suitable for use in an IND (for example, extract plutonium from MOX fuel) and fashion the extracted material into IND components. However, SNM dilution does impose a time and resource burden on the adversary, and therefore, increases the chances for timely interruption of adversary actions and material recovery by law enforcement organizations. The cost of the required materials (e.g., chemicals) and equipment, and, in certain cases, the required scale of processing operations, also increases for dilute materials. Additionally, assembling the IND components and successfully detonating such a device has its own unique challenges for an adversary.

Based on the new information discussed above, the staff concludes that the existing regulations for fixed sites and transportation could be improved and that material attractiveness considerations should be incorporated in the existing material categorization or in a new material categorization. As part of the proposed rulemaking and as discussed further in Section 4, "Basis for Requested Changes," the staff intends to retain the existing material categorization approach and to enhance the effectiveness and efficiency of the graded approach to physical protection by considering the effect dilution has on the attractiveness of forms of nuclear materials in addition to SNM type and quantity. The extent of dilution of SNM by other materials (e.g., SNM in a chemical compound or physical mixture) is critical to determining an adversary's ability to acquire and use the material in an IND. Clearly, because of their greater bulk and weight (and assuming equal levels of protection), diluted SNM are more difficult to steal and easier to recover. Additionally, adversaries would face greater technical, operational, and logistical challenges when conducting SNM processing operations and constructing an IND.

A detailed discussion of classified aspects of the technical basis for the proposed material categorization and attractiveness approach is contained in a separate classified document.

Threshold Dose-Rate Limit

As discussed in Section 2, "Existing Regulatory Framework," an external radiation dose-rate threshold is used in the existing regulations in two ways. In one case (e.g., as addressed in §73.6 and §73.50), the external radiation dose-rate threshold is used to differentiate between irradiated and un-irradiated SNM and to assign physical protection measures for irradiated SNM. In the other case (e.g., as addressed in §73.60), the external radiation dose-rate is considered as a security feature permitting less stringent physical protection (§73.67 versus §73.60). As discussed in Section 2.1, "Regulatory History," the existing external radiation dose-rate threshold was previously considered sufficient to act as an effective deterrent to the unauthorized removal of material. Using external radiation as a security feature is often termed "self-protection." However, based on changes in adversary characteristics (e.g., willingness to sacrifice themselves in order to complete a malicious act) and new technical studies, the continued use of the existing external radiation dose-rate threshold as a security feature might not be prudent or realistic since, in some cases, the adversary may fulfill their goal prior to succumbing to the effects of radiation that may include death.

In 2005, Oak Ridge National Laboratory issued "Radiation Effects on Personnel Performance Capability and a Summary of Dose Levels for Spent Research Reactor Fuels" (ORNL, 2005). This report evaluated the external radiation dose-rate over time and the potential health effects associated with those external radiation dose-rates. The study concluded in part that a 100 rem per hour at 3 feet external radiation dose-rate threshold will not incapacitate an individual for several hours. In the current threat environment and in order to be relied on as an effective security feature, the external radiation dose-rate should be physically incapacitating before an adversary is able to complete a malicious act (i.e., theft or radiological sabotage). The study indicates that an external radiation dose-rate of 4,000 Rad/hour would incapacitate an individual in 60 minutes and an external radiation dose-rate of 10,000 Rad/hour would incapacitate an individual in 30 minutes.

This concept is also considered in INFCIRC/225, Revision 5 (IAEA, 2011). Section 4.6 of INFCIRC/225, Revision 5 (IAEA, 2011) states that "…if the threat assessment or design-basis threat includes an adversary who is willing to perform a malicious act, States should carefully consider whether or not to reduce the categorization levels of the material on the basis of radiation levels sufficiently to incapacitate the adversary before the malicious act is completed."

Based on the above, the staff concludes that the external radiation dose-rate in the existing regulations is not sufficient for use as a security feature but does serve as a reasonable threshold to differentiate between irradiated and un-irradiated SNM.

Sabotage

Physical protection requirements related to irradiated SNM, which might pose a sabotage risk, are addressed in §73.50. As discussed in Section 2.1, "Regulatory History," radiological sabotage was more explicitly considered in Part 73 in the late 1970s when the previous fixed facility requirements were retained in §73.50. The requirements in §73.50 only apply to formula quantities (i.e., Category I quantities) of certain types of strategic SNM. That is, material not

subject to §73.51 that is not readily separable from other radionuclides and which has a total external radiation dose-rate in excess of 100 rem per hour at a distance of 3 feet without intervening shielding.

Since the late 1970's, the way sabotage is defined and considered has evolved. For example, radiological sabotage is defined in 10 CFR 73.2 as "any deliberate act directed against a plant or transport in which an activity licensed under the regulations in this chapter is conducted, or against a component of such a plant or transport which could directly or indirectly endanger the public health and safety by exposure to radiation." In 10 CFR 37.5, sabotage is defined as "deliberate damage, with malevolent intent, to a category 1 or category 2 quantity of radioactive material, a device that contains a category 1 or category 2 quantity of radioactive material, or the components of the security system." While the definition of sabotage in Part 73 is broad, it focuses on acts against a facility or transport. The definition of sabotage in Part 37 focuses on the malevolent use of the radioactive material. Both types of sabotage (e.g., sabotage consequences resulting from malevolent acts on a facility and sabotage consequences resulting from the use of SNM) need to be considered in determining the appropriate physical protection requirements because both types of sabotage can adversely impact public health and safety.

The threat environment since 2001 has highlighted terrorist interest in using radioactive materials, including SNM, in a radiological dispersal device[4] (RDD) or radiological exposure device[5] (RED). The radiation and radiotoxicity levels of certain types and forms of SNM affect their attractiveness for radiological dispersal/dirty bomb or exposure scenarios (e.g., the theft of material for RDDs and REDs that might be used by adversaries). In addition, these materials might not necessarily be, and often are not, above the external radiation dose-rate threshold or contain a Category I quantity of material. This condition results in a regulatory gap whereby the existing regulations might not fully protect material that should be protected to manage radiological sabotage risk and/or risk of the material being used in an RDD.

The U.S. Government has extensively studied the risk of radioactive materials being dispersed by an explosion or other means (RSPSTF, 2010). Based on these studies, the NRC has a greater understanding of the risks and consequences associated with malevolent use of these materials, either at a facility, away from a facility, or during transport. The existing regulations in §73.50 related to protection against sabotage only apply to relatively large quantities of strategic special nuclear material (i.e., Category I quantities (5,000 grams of HEU or 2,000 grams of uranium-233 or plutonium)). A classified Sandia National Laboratories (SNL) study (SNL, 2009) produced estimates of minimum mass of a variety of radionuclides, including SNM, needed to exceed a limiting consequence criteria for various potential terrorist scenario classes (including RDD and RED scenarios). The SNL study indicate that smaller quantities of SNM (predominately plutonium and non-power reactor fuel) could pose a risk to public health and safety if they are used in an RDD. The current regulations related to sabotage risk do not reflect this increased risk associated with SNM being used in an RDD.

---

[4] *Radiological Dispersal Device* is the combination of radioactive material and the means (whether active or passive) to disperse that material with malicious intent without a nuclear explosion. (RSPSTF, 2010)

[5] *Radiation Exposure Device* is an object used to maliciously expose people, equipment, and/or the environment to ionizing radiation without dispersal of radioactive material. (RSPSTF, 2010)

The physical protection requirements to prevent theft or diversion provide some level of protection against radiological sabotage. The dynamics for setting protective measures against radiological sabotage scenarios need to be more coherently described and conveyed to the industry, the public, and other stakeholders. Indeed, the grading scale for radiological sabotage is not always equivalent to that for theft or diversion. For example, plutonium is highly radiotoxic and, therefore, can be both a theft and sabotage target. The radiotoxicity of HEU is not necessarily significantly greater than that of low-enriched uranium, and neither un-irradiated HEU nor LEU is considered a sabotage target.

In 2013, the NRC issued regulations in Part 37 to establish physical protection requirements for the use and transport of Category 1 and Category 2 quantities of radioactive material that are widely used in the United States, typically by industrial, medical, and academic institutions. The theft or diversion of risk-significant quantities of radioactive materials could lead to their use in a RDD or RED. The physical protection of plutonium-238 and plutonium/beryllium sources is addressed by Part 37. However, other plutonium isotopes are not addressed by Part 37. This results in a regulatory gap that will be addressed by this rulemaking.

Also, although commercial light-water spent nuclear fuel is less attractive as a source of SNM for an IND because of its high radiation levels, its highly radioactive fission products make it attractive as a potential radiological sabotage target for adversaries. These materials are required to be protected to a degree consistent with §73.51 and security orders (applicable to spent fuel storage facilities) and §73.55 (applicable to nuclear power reactors).

Sabotage concerns associated with irradiated non-power reactor fuel varies because of the wide variety of power levels, fuel types and operating history at those facilities. In general, un-irradiated HEU non-power reactor fuel would have similar attractiveness as a theft or diversion target as similar quantities of similar HEU material at a fuel cycle facility. Once irradiated in the non-power reactor core, the HEU non-power reactor fuel becomes a sabotage target because of fission products and its radiation dose rate. In general, un-irradiated LEU non-power reactor fuel represents a lesser theft or diversion target, but irradiated LEU non-power reactor fuel does represent a theft and malevolent use target. The existing physical protection requirements against sabotage for non-power reactors in §73.60(f) address sabotage risk at those facilities but those requirement do not provide specific physical protection measures. This lack of specificity in physical protection requirements should be addressed in the rulemaking to increase regulatory stability, predictability and transparency. The non-power reactor sabotage physical protection measures are currently addressed through compensatory measures and confirmatory action letters; and NRC proposes to include these compensatory measures into the regulations.

Safety/Safeguards Interfaces

The need for establishing strong safety/safeguard (i.e., physical protection and MC&A) interfaces has been recognized both domestically and internationally. Currently nuclear power reactor licensees must evaluate the safety/security interface under the requirements in §73.58, “Safety/Security Interface Requirements for Nuclear Power Reactors.” Additionally, in 10 CFR 76.68(a)(3), “Plant Changes”, gaseous diffusion plants have to ensure that changes do not decrease the effectiveness of the plant's safety, safeguards, and security programs. Also, the

IAEA has recognized the importance of this topic through the publication of "The Interface Between Safety and Security at Nuclear Power Plants" (IAEA, 2010). Finally, DOE directives also place greater emphasis on the integration of MC&A and physical protection (DOE, 2005).

The goal of safety is to prevent and mitigate accidents; the goal of physical protection is to prevent intentional acts that might negatively impact the facility or result in the theft or sabotage of nuclear materials; and the goal of MC&A is to (1) maintain current knowledge of the location of SNM and resolve any discrepancies and (2) prevent undetected access resulting in unauthorized changes to values of SNM at a site that might ultimately result in diversion of SNM. MC&A also complements international treaty obligations by accounting for SNM at facilities and reporting the quantity of SNM at those facilities, as appropriate, to the IAEA. Each of the three disciplines shares the common goal of protecting people and the environment.

Based on past fuel cycle facility and non-power reactor operating experience, there have been cases in which changes made at the facility resulted in an unintended change in either the safety or security posture at the facility. In these cases, the licensee did not conduct a full analysis of the proposed change to fully understand the impact of the change on the overall operations of the facility before authorizing its implementation. For example, the installation of a new security barrier might provide the required level of protection against theft of material, but might also prevent the proper operation of the facility.

Fuel cycle licensees are currently required, under 10 CFR 70.72, "Facility Changes and Change Process," to establish a configuration-management system to evaluate, implement, and track each change to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel. Specifically, §70.72(a)(2) requires licensees to ensure, and document in written procedures, that impacts of changes on safety and health or control of licensed material are addressed before implementing any change. While control of licensed material can impact safety, the implementation of that control is related to physical protection and security. The current language of this part is safety-focused and does not explicitly address a facility's security or safeguards program. Also, 10 CFR 70.32, "Conditions of Licenses," and 10 CFR 70.34, "Amendment of Licenses," make clear that prior approval is required for plan changes that would decrease the effectiveness of the physical protection or MC&A programs. However, there is no explicit requirement to determine that changes to one program do not negatively impact the other and/or safety.

Similarly, non-power reactors are currently allowed under 10 CFR 50.59, "Changes, Tests and Experiments," to perform certain activities without obtaining a license amendment. This portion of the existing regulations, however, does not require explicit consideration to determine that changes do not negatively impact safeguards and/or safety programs.

Unlike nuclear power reactor licensees, fuel facility and non-power licensees are currently not required to ensure that any changes to safety functions, systems, programs, and activities do not have unintended consequences on other facility security functions, systems, programs, and activities. As discussed in Information Notice 2005–33, ''Managing the Safety/Security Interface'' (NRC, 2005), changes made to a nuclear power reactor, its security plan, or the implementation of the plan can have adverse effects on safety if the changes are not adequately assessed and managed. Based on the NRC's experience in reviewing licensees' implementation of new security requirements since the terrorist attacks of September 11, 2001,

the staff believes that it is appropriate to adopt requirements similar to those of §73.58 (applicable to nuclear power reactor licensees) for fuel cycle facility and non-power reactor licensees. Additionally, the staff is aware that the increased complexity of licensee security measures now required in the post-September 11, 2001, security environment could potentially increase adverse interactions between safety and safeguards programs. Also, some fuel cycle licensees rely on aspects of their MC&A program to support process controls and items relied on for safety as described in Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material," of Part 70, "Domestic Licensing of Special Nuclear Material." In one instance, the failure of an MC&A measurement function resulted in a shutdown because related items relied on for safety depended on MC&A data. Similar cases have been identified at non-power reactor facilities.

The staff concludes that a more formal program to ensure that fuel cycle facility and non-power reactor licensees properly assess the safety/safeguards interfaces is required in carrying out and managing these changes. The end result would be to give assurance that a single element of the safety or safeguards system, because of an unanalyzed interaction with the other areas, would not impact the mission of those elements. The net effect would enhance defense-in-depth practices by considering and avoiding unintended consequences.

Implementation and Oversight Experience

Implementation and oversight experience also shows the need to modify and clarify several portions of Part 73. The NRC considered lessons learned from inspection and oversight activities of the current regulations and security orders. Oversight activities identified that regulatory language as currently written in some instances has not resulted in the desired actions from licensees. For example, §73.67(d) and (f) excludes Part 50 nuclear power reactor licensees from the requirements in these sections based on the assumption that physical protection requirements in §73.55 would exceed those required for Category II and III materials. However, oversight activities identified that in some cases Part 50 nuclear power reactor licensees have stored and possessed Category II or III materials in the owner-controlled area of nuclear power reactors where the physical protection requirements in §73.55 are not applicable. Therefore, in some cases these materials might not be protected at the levels required in §73.67(d) and (f). The exceptions need to more precisely state that such excepted materials should be located within the protected area of a nuclear power reactor and covered by its security plan.

Also, facilities have carried out the surveillance requirements (two-person rule) in §73.45(d) and §73.46(e)(9) to focus the security organization on potential movement of material out of the material access area. Changes to the existing regulations are needed to more completely deter and detect theft or diversion of SNM within a material access area in addition to SNM leaving the material access area. Furthermore, the existing regulations in §73.46(d)(9) do not clearly articulate what is expected from the two searches of individuals leaving the material access area.

Implementation experience has identified that the current security plan requirements in §73.67(c) for Category III SNM have not resulted in the desired level of regulatory oversight. That is, only Part 70 licensees possessing greater than 10 kg of Category III SNM are currently required to submit a security plan for NRC approval. Part 50 non-power reactor licensees are

currently not required to have a NRC approved security plan. However, the staff believes that greater oversight is required for small quantities of HEU, uranium-233 and plutonium (i.e., Category III quantities) and quantities of uranium enriched above 10 percent, including non-power reactors. The theft or diversion and malevolent use of those materials warrant the submission and approval of a security plan.

Implementation experience has also identified requirements that are imposed by the NRC for other facilities that should be considered in the physical protection of SNM at fixed sites. These include requirements for training, compensatory measures, suspension of security measures, and consideration of unattended openings.

Because SNM transportation physical protection requirements have not been revised in over 20 years, these requirements are not always consistent with the existing operational practices or relevant transportation security requirements issued by other agencies (e.g., Department of Energy/National Nuclear Security Administration). For example, no NRC-licensed shipments of Category I SNM have occurred since the 1980s, and the NRC Category I SNM transportation physical protection regulations have not been used since then. As discussed above, DOE's Office of Secure Transportation currently transports all Category I SNM in the United States. In performing its mission, the DOE Office of Secure Transportation is exempt from NRC's transportation security regulations. However, NRC's security regulations for transport of Category I SNM should be revised to ensure adequate protection in the event the DOE decides not to continue to transport this material.

Implementation experience by other agencies has identified requirements that should be considered in the physical protection of SNM during transport. Considering the physical protection requirements of similar material by other agencies is beneficial to ensure that a commensurate level of protection is provided and to identify and address gaps or vulnerabilities, as appropriate. The existing NRC SNM transportation security requirements are not fully aligned with DOE transportation physical protection policies and orders for similar materials with similar risks. Unlike the NRC, DOE has revised its SNM transportation security requirements to consider the evolving threat post September 11, 2001. For example, the DOE orders for Category I shipments required tracking. A comparison of DOE and NRC SNM transportation physical protection requirements was performed through SNL (SNL, 2013a; SNL, 2013b; SNL, 2013e; SNL, 2013f; SNL, 2013g).

The staff also considered the implementation of transportation security by other agencies in determining whether issues needed to be addressed by this rulemaking. The NRC recognizes other Federal authorities that have promulgated regulatory requirements governing the transportation of hazardous material including SNM. In some cases, these regulatory requirements may also meet NRC regularity standards. For example The Maritime Transportation Security Act of 2002 (MTSA) addresses port and waterway security. This law is the U.S. implementation of the International Ship and Port Facility Security Code (ISPS). Its full provisions came into effect on July 1, 2004. It requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment. The MTSA creates a consistent security program for all the nation's ports to better identify and deter threats. These competent authorities will be taken into consideration during

the rulemaking process and should be considered when licensees are planning and coordinating their security programs. When implementing the proposed access authorization measures, licensees could take advantage of other existing security and identification programs, such as the Transportation Worker Identification Credential (TWIC). The TWIC program is a Transportation Security Administration and U.S. Coast Guard initiative in the United States. The TWIC program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act of 2002, or MTSA, and all U.S. Coast Guard credentialed merchant mariners.

In addition, transportation security technologies and practices have rapidly advanced over the past 10 to 15 years. Global Positioning System tracking, cell-phone communications, and other modern technologies are now a common part of transportation security. Additionally, based on implementation experience from transportation security operations (including those in high-threat areas overseas), the equipment, procedures, and tactics used to protect high-value assets in transit have also changed significantly. This rulemaking seeks to reflect the impact of these new technologies and procedures on SNM transportation security.

International Guidance

Insights were also gained by reviewing international guidance. As part of preparing to host an IAEA International Physical Protection Advisory Service mission to the United States in October 2013, differences between the international recommendations and existing NRC measures for fixed sites were analyzed (IAEA, 2013). The International Physical Protection Advisory Service team concluded that nuclear security within the U.S. civil nuclear sector is robust and sustainable and has been significantly enhanced in recent years. The team identified a number of good practices in the nation's nuclear security regime and made a recommendation and some suggestions for continuing improvement of nuclear security overall. These suggestions and INFCIRC/225, Revision 5 (IAEA, 2011) recommendations will be considered during this process.

Separately, recommendations in INFCIRC/225, Revision 5 (IAEA, 2011) were also assessed against the NRC SNM transport regulations. This was accomplished through a contract with SNL (SNL, 2013c; SNL, 2013d; SNL, 2013h). Numerous differences were identified between the IAEA recommendations and the existing NRC transportation physical protection requirements for all categories of SNM. Minor differences included several internationally recommended definitions for several transport-specific terms. The greatest differences to be considered for all categories of shipments included: international movement-specific measures, intermodal movement measures, planning specifics, location and recovery measures, minimization/mitigation of radiological consequence measures, compensatory measures, configuration management of the physical protection system, provisions for missing or misplaced materials, measures for unauthorized removal integrated with sabotage protection, measures specific to securing packages, and performance testing. In addition, in contrast to the NRC regulations, the international recommendations called for exercise testing of the response force actions for all categories of SNM transport.

3.3 Consistency and Clarity

The third objective of this rulemaking is to improve consistency in the NRC's physical protection regulations, enhance the clarity of the NRC's SNM physical protection regulations, and improve the format and structure of the requirements (flow) to improve the readability of the requirements. Legislative and policy changes, inconsistencies in the use of terms, the level of detail provided for similar regulatory requirements, and inconsistencies in the protection of material of similar risk require that the existing regulations be revised or in some cases enhanced.

The need to improve regulatory consistency and clarity is driven in part by legislative and policy changes. In many cases, the SNM physical protection regulations are written in a manner that is difficult to follow. To be consistent with the Plain Writing Act of 2010, Executive Order 13563, "Improving Regulation and Regulatory Review" (76 FR 3821; January 21, 2011), and the NRC's internal management directives, changes to the existing regulations are required to improve understandability and ease of use by the staff, the regulated community, and other stakeholders. For example, the phrase "formula quantity of strategic SNM" is used to describe Category I material; whereas the phrase "SNM of moderate strategic significance" is used to describe Category II material. Both of these phrases are cumbersome and make the current regulations less understandable and user-friendly. The existing regulations are also difficult to understand because in some cases they mix physical protection requirements for both fixed sites and transit in a single section. For example, the exemptions in §73.6 apply to physical protection for both fixed sites (i.e., §73.45 and §73.46) and in transit (i.e., §73.25 and §73.26) as well as to notification requirements for in-transit material (i.e., § 73.27). But the SNM listed in the exemption is not completely consistent with types of materials covered by all these specific sections. In addition, the security orders (discussed in Section 1, "Background") in some cases contained new requirements which were conceptual rather than specific. Additional clarity in these cases is needed for licensees to more fully understand what is required to meet the regulatory requirements.

Also, the NRC's regulatory philosophy has shifted to be more performance-based. New requirements typically adopt performance-based approaches and are informed by the current understanding of certain risks which the new requirements were meant to address. However, most of the existing SNM physical protection regulations were developed before the implementation of the Commission's Risk-Informed Regulatory Implementation Plan (NRC, 2000a). Consequently, the existing SNM physical protection regulations are, for the most part, prescriptive and deterministic.

Ensuring consistency in the use of terms for similar security concepts throughout Part 73 is another objective of this rulemaking. The NRC completed the Power Reactor Security rulemaking, which updated physical protection requirements for nuclear power reactors in §73.55 (74 FR 13926; March 27, 2009), to include making generally applicable the security-order requirements issued to nuclear power reactors and to make the regulations more risk-informed and performance-based. The existing regulations for both nuclear power reactors and fuel cycle facilities currently describe the same or similar physical protection requirements using different language. For example, the Power Reactor Security rule added a new Section VI, "Nuclear Power Reactor Training and Qualification Plan for Personnel Performing Security Program Duties," to Appendix B, "General Criteria for Security Personnel," of Part 73.

This new Section VI specifies the requirements for the training and qualification plan for security personnel at nuclear power reactors. In the existing regulations, Category I fuel cycle facility security personnel training and qualification requirements are provided in Sections I through V of Appendix B to Part 73 and §73.46. The new power reactor training and qualification plan requirements in Section VI are essentially the same as the existing Category I training and qualification requirements except for a limited number of differences. For example, Section VI power reactor requirements contain additional requirements that include contingency drills, and a Performance Evaluation Program, which are security order requirements. Still other portions of the regulations (e.g., in §73.50) contain similar requirements that are worded differently with varying levels of detail. For example, §73.50(d)(1) discusses how alarm and line supervisory systems shall at a minimum meet a Government Services Administration Interim Federal Specification, whereas similar requirements in §73.46(e)(7) do not cite a specific standard.

The Power Reactor Security rule also established a more user-friendly and transparent framework and structure for physical protection requirements. This structure groups physical protection requirements into subsystems or functional areas of the physical protection system. These functional areas include, but are not limited to, general performance objectives and protective strategy, security plans, security organization, physical barriers, access controls, search programs, detection and assessment, communications and response.

The staff proposes to use a similar function structure for SNM physical protection requirements. The existing SNM physical protection requirements often mix requirements from several functional areas into a single requirement. For example, §73.46(d)(9)[6] mixes access control, training, personnel search and vehicle search into a single requirement. The current regulations for Category III SNM consist of four requirements. As such, the current regulations for Category II and III SNM do not address all aspects of a physical protection program. For example, the assessment function is not described in the current Category III requirements; and maintenance and testing functions are not described in the current Category II or III requirements. In addition, items, such as access control devices, badging systems, surveillance, escorting, searches, tamper indication and security organization, are only addressed in Category III regulatory guidance. This makes the existing SNM physical protection requirements more confusing and difficult to implement, to inspect and to understand all the requirements associated with a functional area.

---

[6] 10 CFR 73.46(d)(9) states “The licensee shall control all points of personnel and vehicle access to material access areas, vital areas, and controlled access areas. At least two armed guards trained in accordance with the provisions contained in paragraph (b)(7) of this section and appendix B of this part shall be posted at each material access area control point whenever in use. Identification and authorization of personnel and vehicles must be verified at the material access area control point. Prior to entry into a material access area, packages must be searched for firearms, explosives, and incendiary devices. All vehicles, materials and packages, including trash, wastes, tools, and equipment exiting from a material access area must be searched for concealed strategic special nuclear material by a team of at least two individuals who are not authorized access to that material access area. Each individual exiting a material access area shall undergo at least two separate searches for concealed strategic special nuclear material. For individuals exiting an area that contains only alloyed or encapsulated strategic special nuclear material, the second search may be conducted in a random manner.”

The staff believes having similar physical protection requirements associated with a functional area grouped together improves understanding by applicants, licensees and regulators. The staff views the new structure as a more explicit and clear portrayal of the physical protection expectations. In addition, the existing regulations separate out performance objectives from the physical protection requirements. This has resulted in implementation issues resulting in uncertainty regarding what licensees are required to accomplish in both license submittals and inspections. In the nuclear power reactor framework, specific performance objectives for the functional areas are the first item in the group of requirements for a functional area. This approach provides value in being both performance-based, which enhances licensee flexibility in implementing its physical protection program, and clear, which improves understanding of what is required by the SNM physical protection program by applicants, licensees and regulators. This approach will also allow the rulemaking to be applied to future. The new structure is consistent with the material-based approach and provides consistent level of protection for various facility types.

In addition, the existing physical protection requirements in the regulations are sometimes based on material category and sometimes based on specific facility type. Protecting material in different ways depending on the type of facility where the material is located at has, in some cases, resulted in inconsistent protection of material of similar risk. For example, non-power reactor physical protection requirements in §73.60 cite the requirements in §73.67 for Category II and III materials and have additional requirements specific for Category I materials which are different than those in §73.46. Also, Subsection §73.55(l) of the Power Reactor Security regulations provides additional physical protection requirements for un-irradiated mixed-oxide fuel assembles containing a Category I quantity of plutonium dioxide at nuclear power reactors. These requirements and others for nuclear power reactor security, while protecting the un-irradiated mixed-oxide fuel, are not directly consistent with the protection requirements described in the existing regulations for similar material.

The lack of consistency and clarity in the current regulations could result in inconsistent physical protection of the same material at different facilities. These inconsistencies within and among the physical protection regulations increase complexity, decrease understandability, and decrease transparency. This rulemaking, by increasing the clarity and consistency of the NRC's security regulations, will address these issues.

3.4 Use of a Risk-Informed and Performance-Based Structure.

The fourth objective of this rulemaking is to use risk-informed and performance-based approaches and structures. In some cases the security orders and the existing regulations imposed very prescriptive requirements. Similar to the approach used in the Power Reactor Security Rule (74 FR 13926; March 27, 2009), the staff proposes to change the requirements to be more performance-based; that is, to adopt a regulatory approach that focuses on desired, measurable outcomes rather than prescriptive processes, techniques, or procedures. Performance-based regulation leads to defined results while providing licensees with flexibility on how those results are to be obtained. Risk-informed is an approach to decision-making in which risk insights are considered along with other factors such as engineering judgment, safety limits, and redundant and/or diverse safety systems. Such an approach is used to establish requirements that better focus licensee and regulatory attention on design and operational issues commensurate with their importance to public health and safety (NRC, 20114c). The

combined regulatory approach of risk-informed and performance-based regulation would give licensees flexibility in crafting an appropriate security regulatory structure for physical protection of SNM and would provide clear and objective performance standards.

4. Basis for Requested Changes

This section explains the desired changes and discusses the technical rationale and assumptions used to support the recommendations. It also discusses how the requested changes in the regulations can resolve the issues discussed in Section 3, "Regulatory Problem." Where appropriate, this section includes discussions of known legal and policy issues. It explains why certain definitions are no longer adequate and how a revised definition can address the issue. At a high level, this rulemaking proposes the following changes to the regulations: (1) revise the current categorization approach to include material attractiveness, (2) restructure fixed-site and in-transit physical protection to match the new categorization approach, and (3) add other new measures to enhance physical protection based on security orders, risk insights, and implementation and oversight experience gained since 1979.

Changing from a combination of physical protection requirements for three categories of SNM and specific facility types to physical protection requirements based on a material-categorization approach that accounts for risk insights discussed above will result in applying the same or similar physical protection measures for material of similar risk. This will necessitate changes in the structure of Part 73. **The staff proposes to create new subparts and relocate the fixed-site physical protection requirements to one of the new subparts and to relocate the in-transit physical protection requirements of SNM to the other new subpart.** These newly created subparts would be further delineated into performance objectives, capabilities, and requirements for each of the categories of SNM. Conforming changes to move away from facility-based requirements and toward material-based requirements are also considered.

4.1 Material Categorization and Attractiveness

To resolve the issues discussed in Section 3, "Regulatory Problem," regarding material attractiveness, **the staff proposes to introduce three levels of SNM dilution (i.e., non-dilute SNM, moderately dilute SNM, and highly dilute SNM) and associated performance objectives, protective strategies, and specific physical protection requirements**. The dilution levels are based on the LANL studies. The change is intended to right-size the physical protection requirements by aligning them with the risk-significance of the SNM given its type, its quantity, and the level of its dilution. The factors discussed in Section 3.2, "Risk Insights," along with changes to the threat environment and adversary characteristics, were considered in determining proposed changes to the existing physical protection requirements and in determining the appropriate physical protection measures for Category I – moderately dilute, Category I – highly dilute and Category II – moderately dilute SNM.

The primary underlying assumption behind this proposed change is that the level of dilution, in both liquid and dry-mass mixtures, is highly correlated with technical and operational complexities faced by a potential adversary attempting to steal the SNM (given the same level of security) and construct an IND. Indeed, greater levels of material dilution create a set of progressively greater complexities associated with material acquisition (because of material weight and size) and processing (because of larger equipment and process scales, increased

processing timelines, and higher cost). As a result, more dilute (less attractive) material is easier to protect. Should the material be stolen, it is also easier to recover before the adversaries complete the task of material processing and constructing an IND. Therefore, the protective strategy and physical protection requirements should take into account the properties of the material to allow appropriate levels of protection. A specific set of data and analysis to support the recommendation including the selection of dilution levels is provided in a non-public document.

The proposed change is consistent with the recommendations contained in INFCIRC/225, Revision 5 (IAEA, 2011), an international guidance document regarding the adequacy of physical protection measures for SNM.

The staff's approach to material attractiveness has evolved during the development of this regulatory basis. In 2009, the staff proposed, as a starting point, a categorization scheme similar to the DOE's Graded Safeguards Table (Table 4-1) (NRC, 2009). The approach considered a wide range of material characteristics, including its type, quantity, chemical composition, physical form, isotopic content, concentration, and level of irradiation.

Table 4-1: Material categorization approach in SECY-09-0123

	Uranium-235			
Nuclear Material	Attractiveness Level	Cat. I	Cat. II	Cat. III
Pure Products Metals, fluorides, hydrides (≥70 wt %)	A	≥5 kg	≥1 kg <5 kg	≥RQ* <1 kg
High-Grade Materials Metals, fluorides, hydrides (≥20 wt % and <70 wt %); other compounds (≥20 wt %); solutions (≥25 g/l)	B	≥25 kg	≥5 kg <25 kg	≥RQ <5 kg
Low-Grade Materials Metals and compounds (≥1 wt % and <20 wt %); solutions (≥1 g/l and <25 g/l)	C	N/A	≥50 kg	≥RQ <50 kg
All Other Materials Uranium (<10% U-235); highly irradiated material (≥1,000 R/h @ 1 m); metals and compounds (<1 wt %); solutions (<1 g/l)	D	N/A	N/A	≥RQ
	Plutonium and Uranium-233			
Nuclear Material	Attractiveness Level	Cat. I	Cat. II	Cat. III
Pure Products Metals, fluorides, oxides, nitrides, carbides, hydrides (≥50 wt %)	A	≥2 kg	≥0.4 kg <2 kg	≥RQ <0.4 kg
High-Grade Materials Metals, fluorides, oxides, nitrides, carbides, hydrides (≥20 wt % and <50 wt %); other compounds (≥20 wt %); solutions (≥25 g/l)	B	≥10 kg	≥2 kg <10 kg	≥RQ <2 kg
Low-Grade Materials Metals and compounds (≥1 wt % and <20 wt %); solutions (≥1 g/l and <25 g/l); Pu (≥80 % Pu-238)	C	N/A	≥20 kg	≥RQ <20 kg

All Other Materials Uranium (<6% U-233); highly irradiated material (≥1,000 R/h @ 1 m); metals and compounds (<1 wt %); solutions (<1 g/l)	D	N/A	N/A	≥RQ

* "RQ" = Reportable Quantities for MC&A purposes

The staff presented this approach to domestic and international stakeholders, including industry, non-governmental organizations, and the NRC's counterpart agencies in other countries. The initial stakeholder feedback included concerns about potential inconsistency of the two-dimensional table approach with INFCIRC/225, Revision 5 (IAEA, 2011) and the Convention on the Physical Protection of Nuclear Material (IAEA, 1980). The stakeholders also expressed concerns about the complexity of such an initial approach.

Based on the insights gained from early outreach activities, the staff modified the proposed approach, which does not use Table 4-1. Rather than considering multiple parameters (chemical forms, SNM concentration, etc.) in defining SNM attractiveness, the staff determined that considering only SNM dilution (i.e., concentration) is appropriate. The level of dilution generally corresponds to the difficulty of acquiring and processing SNM. In addition, consideration of dilution is consistent with the factors identified in INFCIRC/225, Revision 5 (IAEA, 2011). Dilution (concentration) is expressed as a "dilution factor" which is defined as the weight of uranium-235, uranium-233 and plutonium divided by the total weight of the SNM material and non-SNM materials which are not mechanically separable from the SNM) for solids. For solutions containing HEU, U-233 or plutonium, the dilution factor would be defined as the grams of uranium-235, uranium-233 and plutonium per liter of solution for liquids.[7] For LEU solutions, the dilution factor calculated for the solid would apply because the attractiveness of LEU in solution is less of an attractiveness concern. For mixtures of uranium-235, uranium-233 and plutonium, the unity rule (i.e., sum of the fractions) would apply in determining the overall dilution factor. Based on the results of the LANL study, the staff developed the following three levels of dilution:

1. Non-dilute material is defined as material with a dilution factor equal to or greater than 20 percent for uranium-235 and equal to or greater than 10 percent for uranium-233 and plutonium. Non-dilute materials include, for example, highly attractive HEU, uranium-233, and plutonium metals and compounds.

[7] For the purpose of this discussion, "mechanically separable" means that separation of SNM-containing material from non-SNM material (container, cladding, mixture, etc.) can be accomplished by a simple mechanical operation that does not require specialized tools or processes and that does not considerably increase the adversary's mission timeline (time-on-target). (Generally, an increase in the mission timeline increases the effectiveness of security response to adversary actions and reduces the probability of the adversary's mission being successful.) For example, fresh fuel pellets can be removed (pushed out) from a pressurized-water reactor (PWR) fuel rod and SNM or MOX powder can be poured out from a storage container. In these examples, SNM is mechanically separable. In contrast, in a case of a typical non-power reactor fuel element, SNM cannot be separated from the aluminum matrix of the fuel without chemical processing. Also, the fuel mixture is mechanically bonded to the aluminum cladding and it cannot be separated from the cladding without chemical and/or complex mechanical processing. In this example, SNM is not mechanically separable.

2. Moderately dilute SNM is defined as material with a dilution factor equal to or greater than 1 percent but less than 20 percent for uranium-235 and equal to or greater than 1 percent but less than 10 percent for uranium-233 and plutonium. MOX and certain research and test reactor fuels, for example, can be considered moderately dilute SNM.

3. Highly dilute SNM is defined as material containing SNM but with a dilution factor less than 1 percent for uranium-235, uranium-233 and plutonium. HEU-contaminated processing waste, for which the recovery of SNM is uneconomic, is an example of highly dilute materials.

The existing NRC material categorization scheme shown in Table 4-2 is unchanged. Licensees would first determine which category the SNM is associated with and then use the dilution factor to determine the appropriate level of physical protection. For each pairing of material category and dilution factor, the staff defined an appropriate protective strategy. For example, for non-dilute Category I material, the protective strategy calls for the protection of the SNM against the threat of theft or diversion DBT and radiological sabotage DBT of §73.1. In contrast, the protection measures for Category I - highly dilute material call for an alternate and less rigorous protective strategy involving timely detection of the material theft and communication of the information to law-enforcement agencies to ensure SNM recovery.

Table 4-2: The NRC's current material categorization table

	Cat. I	Cat. II	Cat. III
Uranium, enriched to ≥ 20% U-235	≥ 5 kg	≥ 1 kg < 5 kg	≥ 15 g < 1 kg
Uranium, enriched to ≥ 10 and < 20% U-235	N/A	≥ 10 kg	≥ 1 kg < 10 kg
Uranium, enriched to greater than natural occurrence and < 10% U-235	N/A	N/A	≥ 10 kg
Plutonium and uranium-233	≥ 2 kg	≥ 0.5 kg < 2 kg	≥ 15 g < 0.5 kg

The proposed approach takes advantage of the existing categorization table, but it also incorporates risk-informed insights to adjust protective measures by applying the concept of SNM attractiveness due to dilution. The approach also appears to be more user-friendly compared to the categorization scheme presented in SECY-09-0123 (NRC, 2009). It is also expected to be flexible enough to accommodate emerging fuel cycle technologies and associated new SNM forms.

The proposed approach also does not necessitate significant changes to the material control and accounting regulations contained in Part 74 because the categorization scheme is not being changed. The NRC published a proposed rule to amend the material control and accounting requirements in Part 74 (78 FR 67225; November 8, 2013). Based on that effort, it was concluded that the NRC can proceed with the Part 74 rulemaking while considering material attractiveness issues and developing the regulatory basis for the Part 73 rulemaking. It is anticipated that the proposed scope of this Part 73 rulemaking will require only minor conforming changes to Part 74. Both the regulatory basis for Part 73 and the published proposed rule for Part 74, refer to the material categories and quantities currently existing in the regulations. Even though there is interdependence between Parts 73 and 74, the staff does not think that a Part 73 rulemaking that may allow a licensee to designate diluted material within an

approved security plan would significantly affect the Part 74 regulations or licensees' approved Fundamental Nuclear Control Plans.

4.2 Fixed Site Physical Protection Changes

Following the proposed changes discussed in Section 4.1, "Material Categorization and Attractiveness," **the staff proposes to add three new sets of physical protection requirements** (i.e., for Category I - moderately dilute, Category I - highly dilute, and Category II - moderately dilute) to the existing three sets of physical protection requirements (i.e., Category I, Category II and Category III). Consistent with Section 4.1, "Material Categorization and Attractiveness," licensees would determine the category of material to be protected and then whether the material satisfies any of the dilution levels. Based on category and dilution, as appropriate, licensees would decide how to implement different physical protection requirements to its facility. For example, licensees could determine that even though they possess both non-dilute and moderately dilute Category I materials that it is not advantageous to protect these materials differently. Conversely, the same licensee could establish different areas for non-dilute forms of Category I material and Category I – moderately dilute material where different protection levels would apply. The requirements would be performance-based by allowing licensees to determine how best to apply the requirements to their facilities. The staff determined it was not beneficial to apply additional levels of dilution to Category II or apply any levels of dilution to Category III because there were not clear delineations in applying even less physical protection beyond that provided for Category II – moderately dilute and Category III materials.

The staff further proposes to change those existing physical protection requirements based on security orders, risk insights, and implementation and oversight experience. As such, **the staff proposes to eliminate existing fixed-site physical protection requirements in §73.40, §73.45, §73.46, and §73.67.** As discussed above, the new fixed-site physical protection requirements would be located in a newly created subpart.

The staff used the LANL study to develop protective strategies for each SNM Category and material attractiveness level. The staff then determined conceptual physical protection actions that would be needed to support each protective strategy. To improve consistency among physical protection regulations in Part 73, clarity of the SNM physical protection requirements, and to use a performance-based approach, the staff proposes to have the structure of the new regulatory requirements, as appropriate, be consistent with the structure developed for the Power Reactor Security Rule (74 FR 13926; March 27, 2009). Restructuring the existing requirements into a consistent framework or structure similar to that used in §73.55 and using performance-based requirements will allow applicants and licensees greater flexibility in meeting the level of protection required by the protective strategies. This new structure groups physical protection requirements into subsystem or functional areas of the physical protection system. These functional areas include, but are not limited to, general performance objectives and protective strategy, security plans, security organization, physical barriers, access controls, search programs, detection and assessment, communications and response. Considering the existing physical protection requirements and those imposed by security orders, the staff subsequently developed a set of physical protection measures for each pairing of SNM Category and material attractiveness.

In general, the actions proposed by the new measures for facilities with Category I and Category III materials are not significantly different from what licensees are currently doing to incorporate security-order requirements (discussed in Section 3.1, “Generic Applicability of Security Orders,”). Because the NRC did not issue Category II security orders to address the new threat environment, there is a significant difference in existing Category II requirements and the proposed measures. Also because the new structure includes a more complete description of the aspects of an effective physical protection program in the regulations, rather than including the description partially in regulatory guides, the proposed changes in Category II and III measures appear on their face to be new and significant. The new structure establishes a clear and concise performance-based structure for the protection of SNM along with the associated benefits. The new structure also enhances protection of SNM by ensuring that all aspects of an effective physical protection program are addressed in the regulations. Moreover, the new structure places the requirements in regulation rather than partially addressing these areas in regulatory guidance. This approach is consistent with NRC’s policy that regulatory guides should, in part, describe acceptable ways to meet the regulations and should not impose requirements beyond those in the regulations.

The proposed measures for theft or diversion of SNM at fixed sites for each category and attractiveness are presented in Attachments 3 through 8. The proposed measures for sabotage of SNM at fixed sites are presented in Attachment 9. Where applicable, a reference to existing regulations is provided at the end of the proposed measures. In addition, proposed measures developed with consideration of risk insights are noted with a “1” and proposed measures developed with consideration of security orders are noted with a “2”.

The following subsection further discusses how the regulatory issues presented in Section 3, ”Regulatory Problem,” are addressed by the proposed measures.

Orders for Interim Compensatory Measures and Additional Security Measures

As discussed in Sections 1, “Background,” and 3, “Regulatory Problem,” the NRC is proposing to make certain provisions of security orders generically applicable in this rulemaking. This will increase agency transparency and regulatory clarity. The proposed changes are consistent with the NRC’s strategic goal (see Section 9, “NRC Strategic Plan”) and ensure adequate protection against theft or diversion scenarios associated with malevolent use of SNM.

In order to assess the effectiveness and costs of the security orders, the NRC performed security assessments to find gaps or deficiencies in security requirements at various licensed facilities. The results of the security assessments were used to confirm the effectiveness of the security orders and to determine whether the NRC should take additional actions to ensure adequate protection of materials and to promote common defense and security. The NRC determined that the security-order requirements, which supplement existing regulatory requirements, provide high assurance that the public health and safety, environment, and common defense and security continue to be adequately protected in the current threat environment. That is, the physical protection requirements imposed by security orders and the existing regulations ensure that licensees carry out a minimum level of physical protection measures to manage the risk of the SNM being used for malicious purposes given the current threat environment. Additionally, as discussed above, making the security-order requirements generically applicable in the regulations will improve regulatory consistency and predictability.

As discussed below, the NRC has considered other risk insights and determined that in some cases additional measures are required to ensure adequate protection of the public health and safety and common defense and security.

The agency's policy is generally to rescind applicable security orders if all of the requirements of the security orders are incorporated in an applicable final rule once the rule has become effective. Alternately, the NRC may relax portions of applicable security orders if only a portion of the security order is addressed by the rule. Licensees that received security orders would be informed which security orders would be rescinded or which portions of a security order would be relaxed. Some requirements of the security orders, because of their sensitive nature, would not be rescinded because they will not have been captured in a rulemaking.

Fixed Site - Theft or diversion

In implementing a risk-informed graded approach, protection measures should be commensurate with the potential consequences of malevolent acts to the public's health and safety or to the common defense and security. Grading the physical protection requirements and explicitly considering material attractiveness places more stringent and robust requirements (i.e., the greatest protection) on protecting SNM that is more readily usable in an IND, and makes the physical protection largely proportional to the ease of converting the SNM into a weapons-usable form. The LANL study provided new insights into the ability of adversaries to acquire and use SNM for malevolent purposes. These and other insights were not considered during the security order development and evaluation.

Considering these insights, **the staff proposes six sets of requirements for fixed sites (i.e., for Category I, Category I - moderately dilute, Category I - highly dilute, Category II, Category II - moderately dilute, and Category III) which include performance objectives, protective strategies, and specific physical protection requirements.** The use of material attractiveness (i.e., dilution) would be up to the licensee. That is, licensees could choose to protect dilute material in accordance with the appropriate physical protection requirements for its Category and attractiveness pair or could choose to protect dilute material in accordance with its Category without considering its dilution. Non-dilute SNM would be protected in accordance with its Category.

While the protective strategies and physical protection measures are similar between some of the new more dilute categories and the categories without considering dilution (e.g., between Category I - moderately dilute and Category II), the staff is proposing to keep the sets of physical measures separate. This will allow greater regulatory flexibility in the future to adjust the physical protection measures for individual categories and attractiveness levels without impacting those for other categories and attractiveness levels. This will also allow guidance documents to be tailored to account for differences in material form, size, etc. between attractiveness levels. The proposed measures for SNM at fixed sites for each category and attractiveness are presented in Attachments 3 through 8.

Because one of the key assumptions in applying the material attractiveness concept using dilution is that the SNM is not mechanically separable, **the staff proposes to require, that in order to use the physical protection requirements for dilute materials, the SNM not be mechanically separable.** "Mechanically separable" would mean that separation of

SNM-containing material from non-SNM material (container, cladding, mixture, etc.) can be accomplished by a simple mechanical operation that does not require specialized tools and/or chemical processing and that does not considerably increase the adversary's mission timeline.

Based on risk insights, and the implementation and oversight experience discussed in Section 3, "Regulatory Problem," the staff is proposing several new or modified measures. These include:

1. **The staff proposes to include language in the regulation that states that the NRC may require, depending on the individual facility and site conditions, alternate or additional measures deemed necessary to protect against theft or diversion.** The evaluation of alternate or additional measures would be done on a case-by-case base and would typically be done at the license application phase. This will allow the NRC to apply risk insights from the LANL study to future facilities and forms of SNM and ensure that adequate protection is provided for materials not explicitly considered in this regulatory basis. The staff does not consider that this approach would be used in lieu of security orders to licensees if the threat environment would substantially change in the future. In addition, such language would allow the NRC to impose classified requirements for certain types and quantities of Category I SNM, currently only in security orders, or to place maximum possession limits as license conditions if appropriate. This would allow the Category I security orders to be rescinded.

2. **The staff proposes to require facilities with Category I material to consider the results of an insider risk analysis in developing and implementing their physical protection program.** The goal of the insider risk assessment is to identify potential credible scenarios for a DBT insider to remove Category I SNM outside the site's protected area as well as to assess the effectiveness of the control measures, including physical protection, MC&A, and process control measures, to prevent SNM theft and to facilitate investigative and SNM recovery activities should the material be lost or stolen. This additional analysis is needed to identify potential scenarios that may not be identified by other means that could result in vulnerabilities in a licensee's implementation of the protective strategy.

3. **The staff proposes to revise the training and qualification requirements for facilities with Category I material.** The training and qualification plan requirements in §73.46 should be consolidated and incorporated into Sections I through V of Appendix B to Part 73. In addition, requirements for performance testing, contingency equipment, and weapons which were contained in security orders should also be incorporated into Sections I through V of Appendix B to Part 73, which are similar to requirements that are currently addressed in Section VI of Appendix B of Part 73.

4. **The staff proposes to delete the requirements in 10 CFR 73.55(l), "Facilities using mixed-oxide fuel assemblies containing up to 20 weight percent plutonium dioxide."** Using material attractiveness, this type of fuel would be considered Category I – moderately dilute. The staff reviewed the proposed measures and determined that the protection provided in §73.55 for low-enriched uranium fuel meets or exceeds those proposed in Attachment 4 for Category I – moderately dilute. Thus, additional

protections beyond those required by §73.55 would not be necessary and the additional burden on licensees using mixed-oxide fuel is not warranted. Not deleting the requirements in §73.55(l) would result in inconsistent physical protection of similar material at different facilities.

5. **The staff proposes to include several new functional areas to the six sets of physical protection measures.** These include security program review, compensatory measures, suspension of security measures, and alternative measures. Especially in a performance-based framework, requiring licensees to periodically review their physical protection programs, and evaluate and assess the effectiveness of those programs, promotes continued adequate protection of SNM. Security features and equipment may become inoperable or degraded over time and would require some form of compensatory measures to maintain adequate protection of the SNM. Therefore, requiring the consideration of compensatory measures during the physical security plan development allows licensees to develop compensatory measures and NRC review prior to the occurrence of such situations. This precludes potential issues during the inspection of compensatory measures and ensures that adequate protection of SNM is provided at all times. Also recognizing that emergency or extreme conditions can occur, allowing licensees to suspend security measures as needed in these conditions to ensure health and safety of its employees is desirable. Lastly, having a regulatory structure for licensee to propose and NRC to evaluate alternative measures to a regulatory requirement is performance-based and allows licensees flexibility in protecting SNM without the regulatory burden of the exemption process.

In keeping with moving towards a material-based approach rather than a mixture of material-based and facility-based requirements, **the staff proposes to eliminate §73.60**. In considering application of a material-based approach to non-power reactors, the staff recognizes that the composition of non-power reactor fuel varies. Regardless of whether the non-power reactor fuel contains HEU or LEU, the contained uranium-235 is diluted with other materials in the fuel matrix. In addition, the radiation levels of non-power reactor fuel vary. For example during the life cycle of a facility, SNM may be contained in 1) un-irradiated fuel, 2) in-core fuel, 3) fuel in cycle (e.g., fuel that has been partially irradiated and is temporally not in the reactor core but would be returned to the reactor core), and 4) irradiated fuel no longer in cycle (e.g., fuel that is no longer used in the reactor core). As such, the risk of malevolent use SNM in non-power reactor fuel varies. Both un-irradiated HEU and LEU pose a theft or diversion concern, while in-core fuel, fuel in cycle, and irradiated fuel pose a facility sabotage or theft and malevolent use concern. These later concerns are discussed in the Fixed Facilities – Sabotage section below. In keeping with the material-based approach, un-irradiated non-power reactor fuel should be protected in accordance with the appropriate set of physical protection measures depending on category and dilution. As such, both un-irradiated HEU non-power reactor fuel and un-irradiated LEU non-power reactor fuel greater than 10 kg of uranium-235 would in general be protected as Category II - moderately dilute. Un-irradiated LEU non-power reactor fuel less than 10 kg would generally be protected as Category III. The staff considers this level of protection to be appropriate for those facilities.

For irradiated HEU non-power reactor fuel, **the staff is proposing to introduce an external radiation dose-rate threshold of 50 Gray per hour at one meter** (5,000 Rad per hour at 3.3 feet) whereby SNM remaining above this threshold would be considered “self-protecting”. That

is, SNM above this external dose-rate would not require physical protection for theft or diversion, and the quantity of SNM above this external dose rate would not be considered in determining the category of protection for a facility using Table 4-2. An external radiation dose-rate of 50 Gray per hour at one meter will incapacitate an adversary and is considered sufficiently high to be an effective security feature. This level of external radiation dose-rate is consistent with the ORNL report (ORNL, 2005) and site-specific Security Assessments for non-power reactors prepared by Sandia National Laboratories for NRC in 2006. The external radiation dose-rate threshold should apply to an individual fuel element. However, supporting guidance should consider the amount of shielding required and the appropriateness of applying the external dose-rate threshold to an aggregated Category I threshold quantity of HEU non-power reactor fuel (i.e., 5 kg uranium-235). As discussed below, non-power reactor fuel above 50 Gray per hour at one meter would still require physical protection to address facility sabotage concerns, as discussed below.

In evaluating the appropriate level and regulations associated with the protection of SNM at non-power reactors, the staff was mindful of Section 104.c of the Atomic Energy Act and Commission policy on utilization and production facilities that conduct research and development activities (namely, to impose only the minimum amount of regulation on these licensees necessary to promote the common defense and security and protect the public health and safety). In general, the proposed changes are consistent with activities that are already being done in order to meet existing regulations, orders, or commitments to the compensatory measures issued in the confirmatory action letters. Studies have shown that certain types of SNM are more attractive than others for theft or diversion, theft and malevolent use and facility sabotage, regardless of where the material is stored. Consistent with the Commissions' statutory responsibility to promote the common defense and security and protect the health and safety of the nation, the staff believes that the proposed changes are necessary to fulfill the NRC's statutory responsibilities.

The staff proposes to change the exception in §73.67 to except SNM located within the protected area of facilities and included in the security plan for nuclear power reactor licensees meeting the requirements of §73.55. This will ensure that any Category III SNM located outside a protected area is adequately and consistently protected.

For Part 73, **the staff proposes to change the following definitions**:

- Eliminate *Formula quantity* and add *Category I quantity* means high enrich uranium, plutonium or uranium-233 in any combination in a quantity of 5,000 grams or more computed by the formula, grams = (grams contained U–235, contained in uranium enriched to 20 percent or more in U–235 isotope) + 2.5 (grams U–233 + grams plutonium).

- Eliminate *Special nuclear material of moderate strategic significance* and add *Category II quantity* means:
  (1) Less than a Category I quantity of special nuclear material but more than 1,000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U–235 isotope) or more than 500 grams of uranium-233 or plutonium, or in a combined quantity of more than 1,000 grams when computed by the equation, grams = (grams contained U–235) + 2 (grams U–233 + grams plutonium); or
  (2) 10,000 grams or more of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U–235 isotope).

- Eliminate *Special nuclear material of low strategic significance* and add *Category III quantity* means:
  (1) Less than a Category II quantity of special nuclear, but more than 15 grams of uranium-235 (contained in uranium enriched to 20 percent or more in U–235 isotope) or 15 grams of uranium-233 or 15 grams of plutonium or the combination of 15 grams when computed by the equation, grams = (grams contained U–235) + (grams plutonium) + (grams U–233); or
  (2) Less than 10,000 grams but more than 1,000 grams of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U–235 isotope); or
  (3) 10,000 grams or more of uranium-235 (contained in uranium enriched above natural but less than 10 percent in the U–235 isotope).

- Eliminate *Strategic special nuclear material.*

- Add *dilution factor* means the weight of uranium 235, uranium-233 and plutonium divided by the total weight of the SNM material and non-SNM materials which are not mechanically separable from the SNM) for solids and as grams of HEU, uranium-233 and plutonium per liter of solution for liquids.

- Add *moderately-dilute special nuclear material* means the material with a dilution factor equal to or greater than one percent, but less than 20 percent for uranium-235 and equal to or greater than one percent but less than 10 percent for uranium-233 and plutonium for solids and ≥1 gram per liter and <25 gram per liter for HEU, uranium-233 and plutonium solutions.

- Add *highly-dilute special nuclear material* means the material with a dilution factor of less than one percent for solids and <1 gram per liter for HEU, uranium-233 and plutonium solutions.

- Add *mechanically separable* means that separation of special nuclear material-containing material from non-special nuclear material (container, cladding, non-nuclear matrix, etc.) can be accomplished by a simple mechanical operation that does not require specialized tools and/or chemical processing and that does not considerably increase the adversary's mission timeline. This does not include chemical separation.

- Add *aggregated* means accessible by the breach of a single physical barrier that would allow access to SNM in any form, including any devices that contain the radioactive material, when the total activity equals or exceeds an SNM category threshold.

- Add *special nuclear material* means (1) plutonium, uranium 233, uranium enriched in the isotope 233 or in the isotope 235, and any other material which the Commission, pursuant to the provisions of section 51 of the act, determines to be special nuclear material, but does not include source material; or (2) any material artificially enriched by any of the foregoing but does not include source material;

The proposed changes address the regulatory issues discussed in Section 3, "Regulatory Problem," and are consistent with the NRC's strategic goal (see Section 9, "NRC Strategic Plan"). Moreover, the new measures in Attachments 3 through 8 ensure adequate protection against theft or diversion scenarios associated with malevolent use of SNM. Table 4-3 summarizes the proposed fixed site physical protection measures.

Table 4-3: Summary of Fixed Site Proposed Measures

	Category I	Category II Category I - Moderately Dilute	Category II - Moderately Dilute	Category III Category I - Highly Dilute
Protective Strategy	– Protect against DBT of theft or diversion and radiological sabotage – Prevent the removal of SNM and other unauthorized activities involving SNM – Insider Mitigation Program – Insider Risk Analysis	– Immediately detect attempts to remove of SNM and provide sufficient delay through the use of barriers and/or armed responders to allow LLEA to promptly recover SNM	– Promptly detect attempts to remove of SNM and notify LLEA to allow recovery of SNM	– Timely detect attempts to remove of SNM and notify LLEA to allow recovery of SNM
Security Plan	– Physical Security Plan – Safeguards Contingency Plan – Training & Qualification Plan	– Physical Security Plan – Safeguards Contingency Plan – Training & Qualification Plan	– Physical Security Plan	– Physical Security Plan
Security Organization	– Implement Program – Management System	– Implement Program – Management System	– Implement Program – Management System	– Implement Program – Management System
Physical Barriers	– Owner Controlled Area – Vehicle Barrier System/blast analysis – Isolation Zone – Protected Area – Vital Area – Material Access Area – Locked Processes – Vault – Hardened central alarm station (CAS)	– Vehicle Barrier System – Isolation Zone – Protected Area – Controlled Access Area – Locked Processes – Vault-type room – Hardened CAS	– Controlled Access Area – Locked Processes – Vault-type room	– Controlled Access Area
Access Controls	– Protected & Material Access Area Access Portals – Limit unescorted access – Access Authorization Program per Part 11 – Controlled Badge	– Protected Area & Controlled Access Area Access Portals – Limit unescorted access – Access Authorization Program Controlled Badge Program – Escort	– Controlled Access Area Access Portals – Limit unescorted access – Access Authorization Program Controlled Badge Program – Escort	– Controlled Access Area Access Portals – Limit unescorted access – Controlled Badge

	Program – Escort Requirements	Requirements	Requirements	Program – Escort Requirements
Search Programs	– Owner controlled area – vehicles – Protected Area – entry (contraband) & exit (SNM – shielding) – Material Access Area – entry and exit (SNM – shielding) – Vault (weapons)	– Protected Area – entry (contraband) & exit (SNM & shielding) – Controlled Access Area – exit (SNM & shielding)	– Controlled Access Area – entry (contraband) random exit (SNM & shielding)	– None
Detection and Assessment	– Protected Area & Material Access Area Intrusion Detection System with UPS – Video Capture – Central Alarm Station – Secondary Alarm Station – Surveillance Program – Protected Area & unoccupied Material Access Area – Periodic Patrols of outside areas – Two person rule in Material Access Area – Illumination	– Protected Area & Vault type room Intrusion Detection System with UPS – Video Capture – Central Alarm Station – Secondary Alarm Station (on-site or off-site) – Surveillance Program – Periodic Patrols of outside areas – Illumination	– Controlled access area monitored with either intrusion detection equipment or by periodic patrols to detect unauthorized penetrations or activities – Vault type room Intrusion Detection System with UPS – Central Alarm Station – Surveillance Program – Periodic Patrols of outside areas	– Controlled access area monitored with either intrusion detection equipment or by periodic patrols to detect unauthorized penetrations or activities – Surveillance Program – Periodic Patrols of outside areas
Communication	– CAS/SAS two-way redundant communication with LLEA – Continuous communication between CAS/SAS and on-site and off-site response force – Non-portable equipment on UPS	– CAS/SAS two-way redundant communication with LLEA – Continuous communication between CAS/SAS and on-site and off-site response force – Non-portable equipment on UPS	– CAS two-way redundant communication with LLEA – Continuous communication between CAS and on-site and off-site response force – Non-portable equipment on UPS	– Two-way redundant communication with LLEA – Continuous communication among security force – Non-portable equipment on UPS

Response	– 10 Tactical Response Team – interrupt and neutralize – Deadly Force – Armed Security Officers – LLEA Liaison – Heightened Security	– Deadly Force – Armed Security Officers – LLEA Liaison – Heightened Security	– LLEA Liaison – Heightened Security	– LLEA Liaison - Heightened Security
Security Program Review	– Annually – Management Review – Issue identification and resolution program Performance evaluation program	– Biennially – Management Review – Issue identification and resolution program	– Biennially – Management Review – Issue identification and resolution program	– Biennially – Management Review – Issue identification and resolution program
Maintenance & Testing	– Required	– Required	– Required	– As appropriate
Compensatory Measures	– In physical security plan (PSP)	– In PSP	– In PSP	– In PSP
Suspension of Security Measures	– Allowed	– Allowed	– Allowed	– Allowed
Records	– Required	– Required	– Required	– Required
Alternative Measures	– Allowed	– Allowed	– Allowed	– Allowed

Fixed Facilities – Sabotage

As discussed in Section 3, "Regulatory Problem," the understanding of consequences associated with sabotage has evolved since the 1970s. The threat environment has also changed following the events of September 11, 2001. Considering relevant national laboratory studies and the level of protection suggested for theft or diversion (discussed above), the staff determined that Category III quantities of plutonium required additional protection beyond that provided for theft or diversion. The NRC determined the appropriate level of protection to manage risk associated with malevolent use of Category 1 and Category 2 quantities[8] of radioactive material (which includes plutonium sealed sources) in Part 37. Therefore, the additional protection measures beyond Category III theft or diversion protection to meet the level of protection provided by Part 37 are provided in Attachment 9. These changes would provide a consistent level of protection for Pu-239 whether the material was contained in a plutonium/beryllium source or in another form. Similar to Part 37, the protection measures in Attachment 9 recognize that individual sources may be below the 250 gram (16 Ci) threshold and would not require protection unless the aggregate quantity exceeded that threshold.

[8] Category I, II and III designate for categories of SNM, while Category 1 and 2 designate categories of radioactive material.

Spent nuclear fuel[9] also poses sabotage risk. The existing regulations use an external radiation dose-rate threshold of 100 rem per hour at 3 feet to, in part, differentiate irradiated and un-irradiated materials. Moreover, the physical protection of spent nuclear fuel is provided in §73.51(see discussion in Section 2, "Background"), and §72.180, "Physical Protection Plan" as well as requirements in security orders issued to those facilities. As such, to reduce confusion of whether spent nuclear fuel should be protected in accordance with §73.50 or other regulations, **the staff is proposing to eliminate the requirements in §73.50.** The staff recognizes that facilities licensed under Part 70 (such as facilities that analyze spent nuclear fuel in hot cells) may possess limited quantities of SNM contained in spent nuclear fuel. **The staff proposes that quantities of spent nuclear fuel greater than 100 grams other than at a nuclear power reactors or locations specified in §73.51 would be protected in accordance with §73.51. The staff proposes to also apply the additional protection measures in Attachment 9 to quantities of spent nuclear fuel less than 100 grams** other than at a nuclear power reactors or locations specified in §73.51**.** The 100-gram limit is consistent with the NRC's spent nuclear fuel transportation requirements in §73.37. These changes would provide consistent level of protection for spent nuclear fuel regardless of its location.

As discussed above, the physical protection requirements for theft or diversion also provide protection against sabotage. The requirements for non-power reactors issued as part of the confirmatory action letters discussed in Section 3.1, "Generic Applicability of Security Orders," address both protection against theft and malevolent use and facility sabotage. The requirements that protect against theft and malevolent use have been incorporated into the Category II - moderately dilute set of measures. The staff considers these measures adequate protection for in-core fuel, fuel in-cycle and irradiated non-power reactor fuel greater than 10 kg. In addition, as discussed above, irradiated HEU non-power reactor fuel would also require physical protection to address sabotage concerns. The staff considers the Category II - moderately dilute set of measures adequate protection for both theft or diversion and theft and malevolent use scenarios. Additionally, based on NRC studies, facility sabotage protection of fuel is required for non-power reactors with power levels greater than 2 megawatts. As discussed in Section 3.2, "Risk Insights," **the staff proposes to specify in the regulations the measures required to address facility sabotage concerns for non-power reactors with power levels greater than 2 megawatts.** These additional protection measures are provided in Attachment 9. Non-power reactors with power levels less than 2 megawatts are considered not to pose a facility sabotage concern associated with in-core fuel. The staff concludes that additional protection beyond that provided to prevent theft or diversion of LEU non-power reactor fuel is not required to manage the sabotage (i.e., theft and malevolent use) concerns.

Providing additional protection for material that poses a greater sabotage risk fills the regulatory gap discussed in Section 3, "Regulatory Problem," and is consistent with the NRC's strategic goal (see Section 9, "NRC Strategic Plan"). Moreover, the measures in Attachment 9 ensure

---

[9] *Spent nuclear fuel* or *spent fuel* means, "Fuel that has been withdrawn from a nuclear reactor following irradiation, has undergone at least 1 year's decay since being used as a source of energy in a power reactor, and has not been chemically separated into its constituent elements by reprocessing. Spent fuel includes the special nuclear material, byproduct material, source material, and other radioactive materials associated with fuel assemblies." [10 CFR 72.3]

adequate protection against sabotage scenarios associated with malevolent use of plutonium, irradiated non-power reactor fuel and small quantities of spent nuclear fuel.

4.3 Transportation Physical Protection Changes

The level of protection for SNM in transit should be comparable to the level of protection of similar SNM at fixed sites. Similar to the physical protection at fixed sites, the protection of SNM against theft or diversion also provides adequate protection against sabotage scenarios. Generally, protection of SNM in transit is a more challenging security task compared to ensuring security of SNM at fixed sites. Similar to physical protection for fixed sites, the staff proposes to change the existing transportation physical protection requirements based on risk insights, and implementation and oversight experience. As such, **the staff proposes to eliminate existing transportation physical protection requirements in §73.25, §73.26, and §73.67.** As discussed above, the new transportation physical protection requirements would be located in a newly created subpart.

Based on the insights from the LANL study, the staff used the same protective strategies for each SNM Category and material attractiveness level for transport as was developed for fixed sites. The staff then determined conceptual transportation physical protection actions that would be needed to support each protective strategy. The staff subsequently developed a set of physical protection measures for each SNM Category and material attractiveness. The overall goal is to ensure that the level of physical protection for SNM in transit is comparable to that for similar SNM at fixed sites.

Similar to fixed sites, **the staff proposes six sets of requirements for transportation (i.e., for Category I, Category I - moderately dilute, Category I - highly dilute, Category II, Category II - moderately dilute, and Category III) which include performance objectives, protective strategies, and specific physical protection requirements.** This approach will allow licensees to choose to protect dilute material at appropriate lower levels. That is, licensees could choose to protect dilute material in accordance with the appropriate physical protection requirements for its Category and attractiveness pair or could choose to protect dilute material in accordance with its Category without considering its dilution. Non-dilute SNM would be protected in accordance with its Category.

Because NRC has not updated its transportation physical protection requirements to account for changes in the threat environment, the rulemaking also seeks a greater degree of alignment between the NRC transportation security requirements and the requirements promulgated by other U.S. Government agencies, as well as the international recommendations of INFCIRC/225 Rev. 5 (IAEA, 2011), both of which considered the evolving threat. In particular, the rulemaking considers and addresses, as appropriate, the differences identified in the Sandia National Laboratories transportation security comparability study reports (SNL, 2013a; SNL, 2013b; SNL, 2013e; SNL, 2013f; SNL, 2013g, SNL, 2013h; SNL, 2013i). Based on risk insights, and implementation and oversight experience discussed in Section 3, “Regulatory Problem,” the staff is proposing several new or modified measures. These include:

1. **The staff proposes to increase the transportation protection measures for Category I materials, such as requiring tactical response personnel; use of a transportation security system that provides resistance and delay; and searching the conveyance**

and escort vehicles prior to shipment. Note that DOE Office of Secure Transportation currently ships all Category I materials and as such no security orders were issued. The proposed changes are needed to provide adequate protection considering the new threat environment if Category I materials were shipped by an entity other that DOE.

2. **The staff proposes to increase the transportation protection measures for Category II materials, such as NRC approval of the security plan, increase in protective strategy to require immediate detection, delay; use of a transportation security system that provides resistance and delay; and an access authorization program.** Note that DOE Office of Secure Transportation currently ships many of the Category II materials and the number of non-DOE Category II shipments is limited. As discussed in Section 3.3, "Consistency and Clarity," NRC has worked with licensees on a case-by-case basis to ensure adequate protection of Category II shipments, and the NRC did not issue security orders for these materials. The proposed changes are needed to provide adequate protection considering the new threat environment.

3. **The staff proposes to require a movement control center for Category II materials for tracking of material during transportation.** Using the concept of defense in depth and redundant systems, a continually manned movement control center would provide tracking the transportation, periodically communicate with the transporter, and if required, coordinate response forces.

4. **The staff proposes to require that licensees or their agents provide for continuous determination of the position of the shipment and communication of the positioning information to the movement control center for Category I, Category I – moderately dilute and Category II materials.** The staff proposes leveraging new technology such as using GPS tracking as a standard practice across designated SNM shipment categories. GPS tracking of valuable cargo has become a standard practice in the transportation industry. This technology can be a valuable security tool and the staff is considering the use of tracking as a security requirement for shipment of certain types of SNM.

5. **The staff proposes to require searching conveyances prior to loading, positively identifying persons receiving custody prior to transferring custody and enhancing communications in route for Category III materials.** These measures were identified in the gap analysis with DOE and IAEA transportation security requirements. The staff determined that these additional measures are necessary and prudent to allow law enforcement to more quickly and effectively respond to a malicious act.

6. **The staff proposes to require licensees, upon notification by an authorized NRC representative, to implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.** The staff proposes leveraging existing US Government resources to inform licensees of potential risk associated with proposed shipments.

7. **The staff proposes to include several new functional areas to the six sets of physical protection measures.** These include security program review, compensatory measures, and alternative measures. Especially in a performance-based framework, requiring licensees to periodically review their physical protection programs, and evaluate and assess the effectiveness of those programs, promotes continued adequate protection of SNM. Security features and equipment may become inoperable or degraded over time and would require some form of compensatory measures to maintain adequate protection of the SNM. Therefore, requiring the consideration of compensatory measures during the physical security plan development allows licensees to develop compensatory measures and NRC review prior to the occurrence of such situations. This precludes potential issues during the inspection of compensatory measures and ensures that adequate protection of SNM is provided at all times. Lastly, having a regulatory structure for licensees to propose and NRC to evaluate alternative measures to a regulatory requirement is performance-based and allows licensees flexibility in protecting SNM without the regulatory burden of the exemption process.

SNM that is transported by the Department of Energy would remain exempt from NRC regulations. The proposed changes will address the regulatory issues discussed in Section 3, "Regulatory Problem," and are consistent with the NRC's strategic goal (see Section 9, "NRC Strategic Plan"). Moreover, the proposed new measures in Attachments 10 - 15 will ensure adequate protection against theft or diversion and sabotage scenarios associated with malevolent use of SNM during transport. Table 4-4 summarizes the proposed transportation physical protection measures.

Table 4-4: Summary Transportation Security Measures

	Category I	Category I - Moderately Dilute Category II	Category II - Moderately Dilute	Category I - Highly Dilute Category III
Protective Strategy	– Protect against DBT of theft or diversion and radiological sabotage – Prevent the removal of SNM and other unauthorized activities involving SNM – Insider Mitigation Program	– Immediately detect attempts to remove SNM and provide sufficient delay through the use of barriers and/or armed responders to allow LLEA to promptly recover SNM	– Immediately detect attempts to remove of SNM and notify LLEA to allow recovery of SNM	– Detect attempts to remove of SNM and notify LLEA to allow timely recovery of SNM
Transportation Security Plan	– Transportation Security Plan – Safeguards Contingency Plan – Training & Qualification Plan	– Transportation Security Plan – Safeguards Contingency Plan – Training & Qualification Plan	– Transportation Security Plan	– Transportation Security Plan
Security Organization	– Implement Program – Management System	– Implement Program – Management System	– Implement Program – Management System	– Implement Program – Management System

Route and notifications	– Description of route in the Transportation Security Plan – Arrangements with LLEA along the route – Advance notification to NRC and receiver – Receiver confirmation – Notification of shipment to NRC and receiver	– Description of route in the Transportation Security Plan – Arrangements with LLEA along the route – Advance notification to NRC and receiver – Receiver confirmation – Notification of shipment to NRC and receiver – Limit on simultaneous Category II shipments	– Description of route in the Transportation Security Plan – Arrangements with LLEA along the route – Advance notification to NRC and receiver – Receiver confirmation – Receiver's notification of receiving – Limit on simultaneous Category II shipments	– Advance notification to receiver – Receiver confirmation – Receiver's notification of receiving
Transportation Security Measures	– Exclusive use closed and locked conveyance – Specially designed transportation security compartment – Continues determination of positioning – Immobilization device and armored cab for road shipments – Tamper indicating devices on containers and compartment – Search of conveyance and escort vehicles prior to loading	– Exclusive use closed and locked conveyance – Specially designed transportation security compartment – Continues determination of positioning – Immobilization device and armored cab for road shipments – Minimal number of escort vehicles for road shipment – Tamper indicating devices on containers and compartment – Search of conveyance and escort vehicles prior to loading	– Closed and locked conveyance; an open conveyance permitted if the SNM package weighs more than 2000 kg – Cargo aircraft for air transport – Tamper indicating devices on SNM containers – Search of conveyance and escort vehicles prior to loading	– Closed and locked conveyance or an open conveyance, if the SNM package weighs more than 1000 kg, or freight container – Cargo aircraft for air transport – Tamper indicating devices on SNM containers – Search of conveyance and escort vehicles prior to loading
Access Controls	– Controlled access for SNM loading and transfer areas, transportation security systems, transportation conveyances, escort vehicles, and SNM containers. – Controlled badge program – Control of keys,	– Controlled access for SNM loading and transfer areas, transportation security systems, transportation conveyances, escort vehicles, and SNM containers. – Controlled badge program – Control of keys,	– Controlled access for SNM loading and transfer areas, transportation conveyances, and SNM containers. – Controlled badge program – Control of keys,	– Controlled access for SNM loading and transfer areas, transportation conveyances, and SNM containers

	locks, and other access control devices – Access authorization program per Part 11	locks, and other access control devices – Access authorization program	locks, and other access control devices – Personnel trustworthiness program	
Movement Control Center	– Movement Control Center – Continuous monitoring of shipment – Written log – Limited unescorted access to Movement Control Center – Resilience to single adversary action	– Movement Control Center – Continuous monitoring of shipment – Written log – Limited unescorted access to Movement Control Center – Resilience to single adversary action	– Designated point of contact	– None
Communication	– Redundant, 2-way secure communications between Movement Control Center – and convoy, and within convoy – Communications between Movement Control Center and shipment personnel and LLEA along the route	– Redundant, 2-way secure communications between Movement Control Center – and convoy, and within convoy – Communications between Movement Control Center and shipment personnel and LLEA along the route	– Periodic two-way communication checks – Ability to contact LLEA	– Periodic two-way communication checks – Ability to contact LLEA
Response	– Armed responders – Tactical response personnel – Deadly Force – Heightened Security	– Armed responders – Tactical response personnel – Deadly Force – Documented number of LLEA responders – Heightened Security	– Immediate investigation upon missed communication check	– Immediate investigation upon non-arrival on time
Export/Import Shipments	– Container receipt upon entry into the U.S. – Protection of shipments while in the U.S.	– Container receipt upon entry into the U.S. – Protection of shipments while in the U.S.	– Container receipt upon entry into the U.S. – Protection of shipments while in the U.S	– Container receipt upon entry into the U.S. – Protection of shipments while in the U.S
Security Program Review	– Annually – Management Review – Performance evaluation program	– Annually – Management Review –	– Biennially – Management Review –	– Biennially – Management Review –

Maintenance & Testing	– Required	– Required	– Required	– None
Compensatory Measures	– In TSP	– In TSP	– In TSP	– In TSP
Records	– Required	– Required	– Required	– Required
Alternative Measures	– Allowed	– Allowed	– Allowed	– Allowed

4.4 Other Changes

This section presents changes affecting access authorization, the external radiation dose-rate threshold, and the safety/safeguards interface. Conforming changes and changes to other sections than those proposed in newly created subparts are also discussed below.

Access-Authorization Security Order

Current regulations only require access authorization for Category I material under Part 11. As discussed in Section 3.1, "Generic Applicability of Security Orders," under the Energy Policy Act of 2005, the Commission made determinations on which materials were significant with respect to public health and safety or the common defense and security. Subsequently, the Commission did not impose by order access authorization requirements for unescorted access to Category III SNM without significant chemical consequences. As discussed previously, orders were not issued for Category II SNM. The NRC has codified access authorization requirements for nuclear power reactors in §73.56 and §73.57 and non-power reactors in §73.57. To resolve the regulatory gap with respect to access authorization, **the staff proposes to add Category II, and Category II - moderately dilute licensees to the list of applicable licensees in §73.57; §73.59; and §73.61**. In addition **the staff proposes to make applicable to licensees possessing the above materials and non-power reactors access authorization measures essentially the same as the requirements in §37.23, §37.25, §37.31, and §37.33** for determining unescorted access to these materials**.** The staff does not consider it necessary to impose access authorization measures beyond those required for a controlled access area to facilities with Category III material other than non-power reactors. As discussed above, because of the sabotage concerns associated with irradiated non-power reactor fuel, the staff considers it appropriate to enhance protection of these materials.

A robust access-authorization program can manage the risk of insiders aiding or accomplishing misuse of SNM for malevolent purposes. Adding Category II and Category II - moderately dilute SNM facilities to the list of licensees required to implement an access authorization program efficiently and effectively meets legislative mandates in the EPAct and Commission policy for determining which licensees should be subject to fingerpringing and criminal history checks. After a final rule is issued and effective, the agency's objective is to rescind the access authorization and fingerprinting security orders issued between 2005 and 2007.

Threshold Dose Limit

The staff considers the 1 Gray per hour at 1 meter dose-rate threshold (100 rad/rem per hour at 3 feet) to be appropriate to distinguish between irradiated and un-irradiated materials. As discussed in Section 3.2, "Risk Insights," relying on the 100 rem per hour at 3 feet external radiation dose-rate threshold as a security feature is no longer deemed prudent. **Therefore, the**

staff proposes to remove and reserve the exemption in §73.6(b). In addition, by eliminating §73.60, the external radiation dose-rate threshold will no longer be used to reduce the physical protection at non-power reactors without consideration of what types of scenarios are need to protect the non-power reactor fuel. As discussed above, the staff considers the use of 50 Gray per hour at 1 meter as an appropriate threshold to distinguish when HEU non-power reactor fuel would not be an attractive target for theft or diversion for use in an IND. These materials would require protection against sabotage scenarios. That level of protection is discussed in the Fixed Facilities – Sabotage section above.

Safety/Safeguards Interfaces

Currently, in §70.72, the NRC requires licensees that possess greater than a critical mass of SNM, and are engaged in certain activities that could significantly affect public health and safety, to evaluate facility changes and the change process from a safety perspective. Likewise in §50.59, non-power reactors have a similar requirement to evaluate changes that effect safety. These requirements were developed because past incidents had demonstrated that some changes made by licensees were not fully evaluated by and/or authorized by facility management and in some cases not fully understood by facility staff. However, the NRC does not require licensees other than nuclear power reactors to assess and manage potential conflicts or impacts between safety and safeguards. As discussed in Section 3, "Regulatory Problem," the staff is aware of instances in which licensee changes in one discipline presented significant potential challenges to another. For that reason, the staff proposes to explicitly require fuel cycle facility and non-power reactor licensees to assess and manage the potential conflicts between safeguards and safety activities. If conflicts or impacts are identified, licensees would be required to take appropriate actions to manage the potential adverse effect. To accomplish this, licensees would need to fully consider safety/safeguard interfaces and coordination, particularly for changes to existing configurations and maintenance.

These proposed measures would require licensees to assess and manage these interactions so that neither safety nor safeguards are compromised. Safeguards and safety programs are complementary in that they both serve the same ultimate purpose of protecting people and the environment from unintended radiation exposure. Therefore, explicitly requiring an interface mechanism will ensure that effectiveness is maintained when changes occur in either safety or safeguards programs.

In keeping with the principles of good regulation, any new measure should minimize the burden on licensees and should allow licensees to make minor changes without NRC approval. As such, the measures should not explicitly require communication to the NRC about the implementation and timing of facility changes beyond those already required elsewhere. The new measures would be intended to promote an increased licensee awareness of the effects of changing conditions and result in appropriate assessment and response to potential or incurred adverse effects. To maintain that awareness, it is proposed that licensees evaluate the effectiveness of their interface evaluations during security-program reviews proposed elsewhere in this document.

During the development of similar reactor requirements in §73.58, the principal concerns expressed by stakeholders were that (1) the proposed §73.58 provisions appeared to require implementation of broad new programmatic requirements, and (2) it did not appear that the

NRC had sufficiently credited existing programs required by the Commission. It is not the intent of this new measure to impose significant new programmatic requirements on licensees. If current programs and procedures are in place to enable the safety/safeguards interface to be assessed and managed, the staff expects that licensees would make maximum use of such programs.

The staff proposes to require safety/safeguards interface measures for Category I, Category I – moderately dilute, Category I – highly dilute, Category II, Category II – moderately dilute, and Category III licensees. The measures should include the following:

> Licensees should (1) assess and manage the potential for adverse effects on safety and safeguards before implementing changes to facility configurations, facility conditions, safeguards, or safety, and (2) where potential conflicts are identified, licensees should communicate them to appropriate licensee personnel and take compensatory and/or mitigating actions to maintain safety and safeguards at the facility.

These interface measures are intended to require licensee evaluation of potential adverse interactions between safety and safeguards activities at facilities during planned or emergent activities. The assessment could be qualitative or quantitative. If a potential adverse effect is identified, the licensee would be required to take appropriate measures to manage the potential adverse effect or make a different change that would not have the adverse effect. The staff recognizes that implementation of these new measures would rely to the extent possible on existing programs that manage facility changes and configuration. Incorporation of these new measures would provide assurance that the safety/safeguards interfaces are considered before changes are made to a facility's current configuration and before new programs or procedures are implemented at a facility.

Conforming Changes

Conforming changes will be required in the following regulations: Part 11; Part 26; Part 50; Part 70; Part 73; Part 76; 10 CFR Part 110, "Export and Import of Nuclear Equipment and Material;" and 10 CFR Part 150, "Exemptions and Continued Regulatory Authority in Agreement States and in Offshore Waters under Section 274".

5. Alternatives to Rulemaking Considered

This section discusses the alternatives to rulemaking that the staff considered to resolve the regulatory issues presented in Section 3, "Regulatory Problem." This section explains why the NRC or the licensees cannot take actions to resolve the issues effectively within the existing regulatory framework. The alternatives considered are described and the reasons why they were not pursued are discussed.

In summary, none of the alternatives resolve or address the regulatory issues or issues with the existing regulatory framework discussed in Section 3, "Regulatory Problem."

5.1 No Action

Under this alternative, the staff would rely on existing regulations, orders, and guidance. Under this alternative, no resources will be necessary for the performance of rulemaking activities. This alternative would require the staff to issue new security orders to new facilities and issue site-specific license conditions to address facility- and SNM-specific risk concerns raised in Section 3, "Regulatory Problem." This alternative has the greatest regulatory uncertainty for new licensees because they would need to design their physical protection systems based on the regulations and issued security orders which may be modified to account for site specific conditions or new threat information. Also, some existing licensees would not fully benefit from potential rightsizing of physical protection requirements discussed in Sections 3, "Regulatory Problem," and 4, "Basis for Requested Changes." This alternative also would not meet the intent of the SRMs discussed in Section 1, "Background." Based on the changes in the threat environment and risk insights discussed above, the staff does not recommend this alternative.

As a variation of this alternative, a non-power reactor licensee further suggested that the scope of the regulatory basis be changed to remove the proposed measures from applying to non-power reactor licensees. The staff considers that adopting a material-based approach has significant advantages over a facility-based approach. Therefore, the staff does not recommend this suggested alternative.

5.2 Issue Generic Communications

There are six types of generic communications NRC could develop and issue. Of these, Bulletins and Generic Letters require a licensee response. Both may request, but not require, licensee action or commitments. The other four generic communications are designed primarily to provide information to licensees.

Regulatory issue summaries are used to (1) document the NRC's endorsement of the resolution of issues addressed by industry-sponsored initiatives, (2) solicit voluntary licensee participation in staff-sponsored pilot programs, (3) inform licensees of opportunities for regulatory relief, (4) announce staff technical or policy positions not previously communicated to the industry or not broadly understood, and (5) address matters previously reserved for administrative letters. *Generic letters* request that addressees (1) perform analyses or submit descriptions of proposed corrective actions regarding matters of safety, safeguards, or the environment and submit, in writing, that they have completed the requests, with or without prior NRC approval of the action; (2) submit technical information that the NRC needs to perform its functions; or (3) submit proposed changes to technical specifications. By a generic letter, the NRC may also (1) provide the addressees with staff technical or policy positions not previously communicated or broadly understood or (2) solicit addressees' participation in voluntary pilot programs.

As the descriptions above suggest, none of these generic communications would be suitable for addressing the large and complex issues described in Section 3, "Regulatory Problem." In addition, regulatory issue summaries and generic letters are tools for existing licensees. While they could be used to raise the awareness of the issues discussed in Section 3, "Regulatory Problem," these generic communications cannot impose new measures or relax existing requirements on licensees. Therefore, this alternative would not be fully responsive to the intent of the SRMs discussed in Section 1, "Background."

5.3 Revise existing regulatory guidance documents

Under this alternative, the staff would issue guidance rather than carry out rulemaking. This guidance would rely on new interpretations of existing regulations to identify desired licensee actions. Pertinent guidance documents are listed in Section 10, “Guidance Documents.”

Regulatory Guides provide guidance to licensees and applicants on acceptable methods for meeting specific parts of the NRC's regulations, techniques used by the staff in evaluating specific issues or postulated accidents, and data needed by the staff in its review of applications for permits or licenses. The NRC issued regulatory guides (RGs) for physical protection of Category I material, and Category II and III materials at facilities in the 1970s and early 1980’s. As discussed in Section 10, “Guidance Documents,” the existing RGs need extensive revision. The magnitude of changes needed to incorporate orders and to risk-inform NRC’s physical protection framework would not allow revisions to regulatory guides alone because RGs cannot impose requirements beyond those in the regulations.

Guidance cannot impose new requirements on licensees, and new interpretations of existing rules are subject to backfit considerations for those licensees that have backfit provisions in their licensing regulations. Also, because regulatory guides cannot mandate licensee action, this alternative is not fully responsive to the intent of the SRMs discussed in Section 1 “Background.”

5.4 Issue New Licensee Guidance

Under this alternative, the NRC could issue new guidance in the form of a new Regulatory Guide or a NUREG. The staff did not pursue this alternative because such documents describe methods that the staff considers acceptable for use in carrying out specific parts of the agency’s existing regulations. As discussed above, because regulatory guides cannot impose requirements on licensees beyond those in the regulations, this alternative is not fully responsive to the intent of the SRMs discussed in Section 1, “Background.”

5.5 Issue Site-Specific License Conditions

Under this alternative, the staff would use a case-by-case evaluation to determine whether the current regulations and orders adequately address potential threats and risk of materials in the license. As discussed in Section 3, “Regulatory Problem,” the NRC has used this approach in the past. This approach could result and has resulted in inconsistencies in protection, and it would create a regulatory burden by requiring the licensees to develop a detailed evaluation of site-specific conditions and risk. The process of developing and implementing individual license conditions can be time consuming and delay the implementation of requirements for the adequate protection of SNM. The staff did not pursue this alternative for these reasons and because it is also not directly responsive to the SRMs discussed in Section 1, “Background.”

As a variation of this alternative, stakeholders suggested grandfathering existing licensees from any changes associated with the rulemaking through license conditions. They noted that the current regulations and security orders recognize the diversity of the small fleet of fuel cycle licensees, allow for a facility-specific risk-informed and performance-based approach, and provide for adequate protection of licensed materials. Any new licensees would be subject to

new measures. This suggested approach appears to be limited to fuel cycle facilities without recognizing other facilities are subject to the existing SNM protection regulations. Most notably, non-power reactors and research facilities are also subject to the existing SNM protection regulations. This approach could result in inconsistencies in protection of similar SNM at different facilities. This suggested approach also does not benefit from the new risk insights. For these reasons and the fact that the suggest alternative is directly responsive to the SRMs discussed in Section 1, "Background," the staff did not pursue this suggested alternative.

6. Backfit Rule Applicability

As discussed in Section 1, "Background," the proposed rulemaking includes updating physical protection requirements for SNM at fixed sites (*i.e.*, fuel cycle facilities, production and non-power reactor utilization facilities licensed under Part 50) to:

- make security requirements imposed by security orders and confirmatory action letters issued following the terrorist attacks of September 11, 2001 generically applicable to fuel cycle facilities, production facilities, and non-power reactor utilization facilities licensed under Part 50
- improve consistency and clarity of physical security protection requirements at fixed fuel cycle facilities
- consider risk-insights from new National Laboratory studies, implementation and oversight experience, and international guidance
- use a risk-informed and performance-based approach
- reorganize and re-sequence regulations to enhance stakeholders' understanding of the NRC's physical protection requirements applicable to fixed sites

This rulemaking will also update requirements governing the transportation of SNM consistent with the new security requirements for SNM at fixed sites, as described above.

Entities who are not provided with backfitting protection

This rulemaking will affect production and non-power reactor utilization facilities licensed under Part 50, all fuel cycle facilities licensed under Part 70, and gaseous diffusion plants who seek or hold a certificate of compliance (CoC) from the NRC under Part 76. Of these entities, only fuel cycle facilities licensed under Part 70, and gaseous diffusion plants who seek or hold a CoC from the NRC under Part 76, are accorded backfitting protection.

Part 50 facilities

Production facilities and non-power reactor utilization facilities licensed under Part 50 are not protected by the Backfit Rule, 10 CFR 50.109. The NRC has determined that the backfit provisions in 10 CFR 50.109 do not apply to production facilities and non-power reactors because the rulemaking record for 50.109 indicates that the Commission intended to apply this provision to only nuclear power reactors, and NRC practice has been consistent with this rulemaking record. Thus, backfitting considerations need not be addressed by the staff in developing the proposed rule as applied to production and non-power reactor utilization facilities

licensed under Part 50. However, the staff will prepare a regulatory analysis that will include consideration of costs and benefits on production facilities and non-power reactor utilization facilities licensed under Part 50.

Part 70 and Part 76 facilities[10]

Fuel cycle facilities licensed under Part 70 and gaseous diffusion plants who have obtained certificates of compliance under Part 76[11] are protected by the backfitting provisions in 10 CFR 70.76 and 10 CFR 76.76, respectively.

Future applicants

Future applicants (of any sort) are not protected by backfitting provisions in 10 CFR 50.109, §70.76 and §76.76 because backfitting is intended to protect the reasonable expectations of certain entities who have received NRC regulatory approvals (*e.g.*, a license), and was not intended to apply to every NRC action that substantially changes the expectations of current and future applicants.

Administrative changes which are not subject to backfitting considerations

Re-sequencing and reorganization of the regulations in Parts 11, 26, 70, 73, 76, 110 and 150 are administrative changes and do not change any underlying substantive regulatory requirement. Therefore, they are not subject to backfitting considerations.

Information collection and reporting

The rulemaking may involve changes to existing information collection and reporting requirements, or the adoption of new information collection and reporting requirements, in Part 73. Information collection and reporting requirements, the primary purpose of which is to support NRC regulatory oversight and is not the achievement of substantive regulatory (radiological health and safety or common defense and security) objectives, are not subject to backfitting consideration. This is a longstanding interpretation of the original Backfit Rule, 10 CFR 50.109, which has been extended to the interpretation of the NRC backfitting provisions in Parts 70, 72 and 76. The rationale underlying the NRC interpretation is that information collection and reporting requirements would be difficult to characterize as involving adequate protection, and usually do not directly result in improvements to radiological health and safety or

[10] The rulemaking will not affect Part 70 licensees who are also nuclear power plant licensees under Parts 50 or 52 at the same site where licensed materials are used. Accordingly, the special considerations which apply to such rulemakings are not applicable to this rulemaking.

[11] The definition of backfitting in 10 CFR 76.76 does not expressly indicate when backfitting protection begins for a gaseous diffusion plant, *i.e.*, when the changed or new NRC position must occur for it to be considered backfitting. Arguably, the lack of a specified action or occurrence marking the start of backfitting protection may be interpreted as reflecting a Commission determination that backfitting protection began when the NRC first adopted § 76.76. To date, neither the staff nor the Commission has been presented the opportunity to directly consider the issue.

common defense and security. Hence, the NRC would likely be unable to justify the adoption of new or changed information collection and reporting requirements under the NRC's backfitting provisions.

Codification of requirements in Orders

Adoption of new or revised regulations which make generically-applicable ("codify") existing requirements in security orders issued to fuel cycle facilities does not constitute backfitting. Backfitting concerns were addressed as part of the NRC's issuance of those security orders, so regulations which codify the existing security order requirements need not be treated as NRC action falling within the definition of backfitting. However, to the extent that the new regulations impose additional or substantially changed requirements which cannot be satisfied by a *current* licensee's/certificate holder's programs and activities, then those additional or changed requirements would be considered backfitting for existing entities. For such requirements, the NRC would address the applicable backfitting provisions.

Revising regulatory requirements to adopt performance-based approach

A significant portion of the rulemaking involves the conversion of current prescriptive requirements to more performance-based requirements. To the extent that existing licensees and certificate holders may be deemed to be in compliance with the revised, performance-based requirements, then those performance-based requirements may be able to be treated as a "voluntary relaxation." A voluntary relaxation exists when the revised or new regulatory requirement may be met by an existing licensee without any change to its existing programs, activities, or design (including the NRC-approved bases for the design). Because the new or revised requirement constituting a voluntary relaxation does not impose a backfitting change on the licensee, the NRC does not consider the adoption of the voluntary relaxation to be backfitting. However, if there are performance-based requirements which are not reasonably regarded as voluntary relaxations, then those requirements will have to be considered under the applicable backfitting provisions, as described below in "Requirements not falling into any of the categories of backfitting rationales."

The staff is considering developing new regulatory requirements which a licensee may voluntary select in lieu of complying with existing unchanged (from a substantive standpoint) requirements, or as an alternative to new or revised requirements which are a "voluntary relaxation." A voluntary alternative exists when a regulation provides two or more alternative regulatory requirements (*e.g.*, alternative A or B, either of which must be selected). Because the new or revised requirement constituting a voluntary alternative does not mandate the licensee to select the newly-adopted alternative requirement, the NRC does not consider the adoption of the voluntary alternative to be backfitting.

Requirements not falling into any of the categories of backfitting rationales

For the proposed regulatory revisions that do not fall into any of the above categories of backfitting rationales, the staff would need to develop the information necessary to address applicable backfitting requirements in 10 CFR Chapter I in developing any proposed rule. In some cases, one of the exceptions from the requirement to conduct a backfit analysis might apply. In other cases, the staff would need to perform a backfit analysis to determine whether

the applicable option would result in a substantial increase in the overall protection of the public health and safety or the common defense and security and determine that the costs of implementing that option would be justified in view of this increased protection.

7. Stakeholder Interactions

This section discusses stakeholder interactions or other outreach efforts that were conducted during the development of this draft regulatory basis document. It also summarizes stakeholder interest and views on the draft regulatory basis.

Staff interacted with licensees, members of the public, other Federal agencies, and representatives of foreign governments, to obtain supporting information, views and opinions on the draft regulatory basis. Affected licensees include fuel cycle facilities, non-power reactors, and other NRC licensees that possess special nuclear material (SNM). Stakeholder interactions are listed in Attachment 1. The outcomes of these interactions are discussed further below. To increase stakeholder involvement and awareness, the NRC used the following additional channels to obtain stakeholder feedback:

1. Since 2011, the NRC solicited feedback through a Web page dedicated to this rulemaking effort (see http://www.nrc.gov/security/domestic/phys-protect/reg-initiatives/10cfr73.html).

2. The NRC held a series of workshops in the February through May 2014 timeframe to obtain stakeholder feedback on the major topical areas being considered for revision in the draft regulatory basis document.

3. The NRC issued a draft of the regulatory basis for public comment in a *Federal Register* Notice ((79 FR 34641; June 18, 2014 and 79 FR 42474; July 22, 2014).

4. The NRC held three announced public meetings on the regulatory basis to obtain public comments on June 12, 2014, September 17, 2014, and September 24, 2014.

External Meetings on Material Attractiveness

Staff conducted extensive outreach with other Federal agencies, the domestic industry, non-governmental organizations and foreign governments about its intent to consider material attractiveness during the revision of the current physical protection measures. The discussion with foreign governments focused primarily on whether staff's approach of considering material attractiveness when revising the necessary physical protection measures for SNM would be consistent with the principles in the INFCIRC/225, Revision 5 (IAEA, 2011). Staff met with six foreign government counterparts to discuss NRC's material attractiveness approach. In all cases, the feedback from representatives of these governments was that the initial technical approach, including the analysis conducted by Los Alamos National Laboratory (LANL), would meet the intent of INFCIRC/225, Revision 5 (IAEA, 2011). However, to assure clarity about meeting the intent of INFCIRC/225, Revision 5 (IAEA, 2011), it was also suggested that the NRC should retain the existing material category table from INFCIRC/225, Revision 5 (IAEA, 2011) and discuss different security measures, adjusted for attractiveness, in the text of the regulation.

Discussions with the domestic fuel cycle, non-power licensees and Nuclear Energy Institute (NEI), focused on gaining an understanding of the potential benefits and impacts on licensees resulting from the adoption of a material attractiveness approach for the physical protection of SNM. Licensee concerns were considered during the development of this regulatory basis document.

Discussions with non-governmental organizations (in particular, the Union of Concerned Scientists and the Belfer Center) highlighted a concern that dilute materials might contain large quantities of plutonium or highly enriched uranium, and hence could still make it possible for an adversary to steal sufficient material to construct an IND. The concerns were also formally submitted and evaluated during the draft regulatory basis document comment period.

NRC Public Workshops at NRC Headquarters

The staff held a series of workshops during the initial formulation of the draft regulatory basis. These were held on February 6, 2914 (Sapountzis, 2014a), February 20, 2014 (Sapountzis, 2014b), April 9, 2014 (Sapountzis, 2014c), and May 28, 2014 (Sapountzis, 2014d). The workshops provided early information on various aspects of the regulatory basis to stakeholders and an opportunity for stakeholders to express views and ask questions. Staff considered the feedback from these workshops in the preparation of the draft regulatory basis document.

NRC Public Meetings at NRC Headquarters

The staff held three announced public meeting on the draft regulatory basis on June 12, 2014 (Sapountzis, 2014e), September 17, 2014, (primarily with RTRs licensees) (Sapountzis, 2014f) and September 24, 2014 (Sapountzis, 2014g). The goals of these public meetings were to inform stakeholders on the different aspects of the draft regulatory basis in order to support the formulation of comments by stakeholders, and to obtain additional stakeholder feedback. NRC transcribed these meetings in order to more accurately capture comments and discussion.

Comments on the Draft Regulatory Basis

The NRC issued the draft regulatory basis (NRC, 2014a) for comments via *Federal Register Notices* (79 FR 34641; June 18, 2014 and, 79 FR 42474; July 22, 2014). The comment period for the document closed on October 17, 2014. A list of commenters is provided in Attachment 2. The following summarizes the comments the NRC received and how they were considered.

Alternatives

Several stakeholders believed NRC should consider an option of grandfathering current licensees. This would include requiring current licensees via a license condition to implement the current regulations and security orders for existing licensees. New licensees would be required to meet any new measures associated with this rulemaking. As a result, staff added this option as an additional alternative to Section 5, “Alternative to Rulemaking Considered.” This alternative was not further considered because this approach could result in inconsistencies in protection of similar SNM at different facilities. This suggested approach also does not benefit from the new risk insights.

Part 74

Comments were received pertaining to the timing of the Part 73 rulemaking relative to the ongoing rulemaking to amend the NRC's material control and accounting (MC&A) regulations for SNM in Part 74. The NRC published a proposed rule to amend the MC&A measures on Part 74 (78 FR 67225; November 8, 2013). The staff does not foresee a problem with proceeding with the Part 74 rulemaking while considering material attractiveness issues and developing the regulatory basis for the Part 73 rulemaking. The NRC does not currently anticipate that a future Part 73 rulemaking with a scope similar to that presented in the draft regulatory basis will require other than conforming changes to Part 74. Both the regulatory basis for Part 73 and the published proposed rule for Part 74 refer to the material categories and quantities existing in the current regulations. The Part 73 regulatory basis further considers the possibility that a licensee may designate diluted material within an approved security plan; however, this would not significantly affect the Part 74 regulations. The staff recognizes the interdependence between Parts 73 and 74; thus, as these rulemakings progress, we will monitor the activities to ensure appropriate coordination.

Clarity and Consistency

Many stakeholders asked for clarifications regarding the intent of a measure or the meaning of particular words or phrases. The level of detail requested in many cases goes beyond that available, or appropriate, at the regulatory basis phase of rulemaking. That is, the information in the regulatory basis is intended to provide staff with concepts of what needs to be changed in the regulations and how identified issues should be resolved. The regulatory basis does not include either rule text or associated guidance. As such, these items would be more appropriately considered as staff develops specific rule text and draft guidance. The comments, while extremely helpful and insightful, will be considered during the proposed rule phase.

Other comments suggested revising or deleting certain measures. While staff evaluated these comments, suggested changes were not incorporated in this document because staff viewed that the measures were needed for adequate protection of the SNM or that the perceived benefit of the measure outweighed the perceived burden.

Several editorial comments were provided and considered in developing the final regulatory basis. Other comments identified areas in the draft regulatory basis where additional clarity was needed. For example, fuel cycle and non-power reactor licensees questioned the applicability of Table 4-1 to staff's proposed changes and in general noted that Table 4-1 was difficult to understand. The staff added additional discussion to Section 4 to clarify the proposed categorization scheme and the application of material attractiveness. Staff further clarified that Table 4-1 was presented for context regarding the initial approach staff considered and how staff's views have evolved during the development of this regulatory basis. Staff believes the inclusion of Table 4-1 illustrates the progression in staff's view and highlights the benefits of staff's proposed approach.

Several comments were provided at the September 24, 2014, public meeting regarding the relative importance of consistency with respect to the other regulatory problems discussed in

Section 3, “Regulatory Problem.” The staff reordered the document objectives by order of importance in Section 1, “Background,” and in Section 3, “Regulatory Problem.”

Regulatory Structure

In response to comments from fuel cycle and non-power reactor licensees questioning the benefit and need for adopting a consistent physical protection regulatory structure, staff added additional discussion to Section 3.3, “Consistency and Clarity,” to clarify the need for the proposed changes. The added discussion was also in response to comments made at the September 24, 2014, public meeting over confusion of whether consistency was being sought for physical protection among licensees. Some stakeholders viewed an approach that sought consistency in physical protection among sites as contrary to performance-based regulation. Staff agrees that the draft regulatory basis was not clear. Staff clarified that consistency in measures and the structure of those measures related to the regulations themselves rather than how the regulations were implemented by a licensee.

Several fuel cycle and non-power reactor licensees questioned the benefit and need for adopting a consistent physical protection regulatory structure. As a result, staff added additional justifications to Section 4.2, “Fixed Site Physical Protection,” regarding the new physical protection measures structure. Staff believes the proposed new structure includes a more complete description of the aspects of an effective physical protection program in the regulations, some of which had been on conveyed in regulatory guides without corresponding measures in the regulations. Because the existing SNM physical protection requirements often mix measures from several functional areas into a single requirement, they can be confusing and difficult to implement, and difficult to inspect. In addition, it is difficult to understand all the measures associated with a given functional area. The proposed new structure groups physical protection measures into subsystem or functional areas of the physical protection system. The proposed new structure is intended to be more user-friendly and transparent.

In response to comments from fuel cycle and non-power reactor licensees regarding the need to identify new measures, staff added additional justifications regarding the new measures for security program review, compensatory measures, suspension of security measures, and alternative measures to Section 4.2, “Fixed Site Physical Protection Changes.” Staff also elaborated on discussions in Section 4.3, “Transportation Physical Protection Changes,” to highlight new measures.

Material Attractiveness

Some stakeholders questioned the general concept of material attractiveness. These comments covered the spectrum from questioning the need for the rulemaking (concluding it may inappropriately reduce physical protection for some forms of SNM) to determining there were benefits to applying material attractiveness and proposing adjusting physical protection measures, accordingly. The staff concluded that the material attractiveness concept should remain as part of the proposed rulemaking, based on evaluations of current sensitive or classified studies that considered information available about adversary capabilities to utilize different forms and concentrations of SNM for use in an IND.

In response to comments from non-power reactor licensees regarding the attributes used to determine material attractiveness, staff revised several definitions and added additional text to clarify how material attractiveness should be considered. Stakeholders noted that "weight percent," as used in the draft, was confusing to non-power reactor licensees because of its use in their technical specifications. As a result, staff proposed using "dilution factor" rather than "weight percent" to quantify different levels for physical protection of less attractive materials. Staff also revised text to clarify how to calculate the "dilution factor" for both solids and solutions, and for mixtures of SNM isotopes.

Several stakeholders believed the document would benefit from additional discussion of the new risk insights and what information or views had changed from the basis used for the existing regulations. Recognizing that much of that information is sensitive and/or classified, staff added limited additional discussion to Section 3.2, "Risk Insights," and Section 4.1, "Material Categorization and Attractiveness," to provide (to the extent possible in an unclassified document) a more detailed explanation of factors affecting material attractiveness.

RTR Fuel Risk

Several non-power reactor licensees noted the draft regulatory basis description of the potential risk from the malevolent use (i.e., theft or diversion, theft and malevolent use, and facility sabotage) of the various types of non-power reactor fuel was insufficient. As a result, staff added additional discussion regarding non-power reactor sabotage to Section 3, "Regulatory Problem." Specifically, the attractiveness of the various types of non-power reactor fuel over its life cycle as a sabotage target was discussed. The discussion touched upon when non-power reactor fuel could be a theft or diversion target, a sabotage target, or both. To more fully address these issues, staff added additional discussion and justification regarding non-power reactor physical protection for theft, diversion and sabotage to Section 4.2, "Fixed Site Physical Protection Changes." The non-power reactor fuel life cycle was described, and physical protection measures commensurate with its risk of malevolent use were assigned. Staff also revised its approach regarding non-power reactor facility sabotage. Facility sabotage measures, currently required by confirmatory action letters and §73.60(f), were described and specifically included as proposed measures.

Several comments from the non-power reactor licensees questioned the proposed elimination of the external dose-rate threshold in the draft regulatory basis. They noted that this would cause some non-power reactor licensees to require Category I – moderately dilute protection and that such protection would be overly burdensome or result in the need to close those facilities. Staff agrees that that level of protection is not appropriate or consistent with the risk significance of those facilities. As a result, staff evaluated what external dose-rate level would be appropriate to preclude the need for higher levels of protection against theft and added additional discussion and justification to Section 4, "Basis for Requested Changes." Specifically, staff revised its approach and proposed an external dose-rate threshold of 50 Gray/hour at one meter. This external radiation dose-rate threshold is considered sufficiently high to be an effective security feature and mitigate theft scenarios. Staff held additional discussions with affected licensees to verify that staff's revised approach addressed stakeholder issues and was implementable.

In response to comments from non-power reactor licensees questioning the consistency of the proposed physical protection changes with the requirements of Section 104.c of the Atomic Energy Act, staff added additional discussion and justification to Section 4.2, “Fixed Site Physical Protection Changes.” In general, the proposed changes are consistent with activities that are already being done in order to meet existing regulations, orders, or as commitments to the compensatory measures issued in the confirmatory action letters. The staff believes that the proposed changes are necessary to fulfill the NRC’s statutory responsibility to promote the common defense and security and protect public health and safety.

Sabotage

In response to comments from fuel cycle and non-power reactor licensees regarding inconsistencies in the proposed approach for additional sabotage protection for Category III quantities of plutonium and the regulatory requirements in Part 37, staff revised the proposed thresholds of such materials to align with Part 37. In revising the sabotage protection of Category III quantities of plutonium, staff identified the need to provide additional clarification regarding the protection of spent nuclear fuel at other than storage and reactor locations for both greater than 100 grams and less than 100 grams to Section 4.2, “Fixed Site Physical Protection Changes.” Staff added justification and measures for various aspects of fuel at non-power reactors including adding specific measures for facility sabotage at non-power reactors with power levels greater than two megawatts.

Safety/Safeguards Interface

Fuel cycle and non-power reactor licensees commented on potential unintended consequences of placing safety/safeguards interface measures in §70.72 and §50.59. Stakeholders noted that an insertion in §70.72 might result in other evaluations required by §70.72 for items relied on for safety being performed in addition to a consideration of safety/safeguards interfaces. That was not the intent of the proposal. As a result, staff modified its approach in Section 4.2, “Fixed Site Physical Protection Changes,” to clarify the intent to be a consideration of possible adverse interactions utilizing existing programs to the extent possible and proposed measures separate from those sections of the regulations.

Fixed Site Measures

Staff made several revisions to the proposed fixed site measures in Attachments 3 through 9 based on stakeholder suggested edits. In general, these changes make the measures more performance-based and should increase clarity.

Several fuel cycle and non-power reactor licensees questioned the proposed measure for certain licensees with Category III material to have security plans and that those plans be approved by the NRC. As a result, staff added additional discussion to Section 3.2, “Risk Insights,” to clarify the need for the proposed changes. The staff believes that greater oversight is required for small quantities of HEU, uranium-233 and plutonium and quantities of uranium enriched above 10 percent, including non-power reactors. The theft or diversion and malevolent use of those materials warrant the submission and approval of a security plan.

Several fuel cycle licensees questioned the proposed changes for additional training of security officers at facilities with Category II – moderately dilute and Category III materials, if those security officers are armed. Based on comments, staff considered that new training measures could result in licensees deciding to unarm security officers that they had voluntarily armed. As a result, staff revised its approach and removed this proposed measure from the regulatory basis.

Several fuel cycle facility licensees commented on the wording associated with having a corrective action program or security event log. As a result, staff revised the text to be performance-based and focus on what the outcome of using these types of documents would achieve without stating what type of documents should be used.

Several non-power reactor licensees commented on the search measures for Category II – moderately dilute SNM. As a result, staff revised the text to be performance-based with respect to the form of the SNM and means of access rather than requiring a search of all individuals regardless of the facility characteristics.

Several non-power reactor licensees commented that certain assessment measures for Category II – moderately dilute and Category III SNM could be overly burdensome. As a result, staff revised the text to remove the measure for a secondary alarm station for Category II – moderately dilute. Staff also revised the need for continuous staffing at the facility for both Category II – moderately dilute and Category III SNM. These changes reduce potential licensee burden while providing protection of the SNM commensurate with its protective strategy.

Transportation Security Measures

Staff made several revisions to the proposed transportation security measures in Attachments 10 through 15 based on stakeholder suggested edits. In general, these changes make the measures more performance-based and should increase clarity.

Several fuel cycle licensees commented on the incorporation of best practices, such as GPS, into the proposed measures. GPS has become routine practice on domestic shipments; however, the use of GPS may not be practical during international transport. As a result, the staff clarified that GPS is proposed to be required for Category I, Category I – moderately dilute, and Category II shipments within the U.S.

Fuel cycle licensees commented that requiring closed and locked conveyances for shipments greater than 2,000 kg will prohibit bulk shipments, add unnecessary costs, and appeared arbitrary. The wording in the draft regulatory basis was confusing with respect to when material could be shipped via open conveyances and when material should be shipped in closed conveyances. Staff agrees that requiring closed and locked conveyances for shipments greater than 2,000 kg is impractical. As a result, staff clarified the wording in the final regulatory basis and also lowered the value to allow open shipments over 1,000 kg for Category I – highly dilute, Category II – moderately dilute and Category III material.

Fuel cycle licensees commented that the measures for Category III shipments appear to exceed the licensee's authority and capability to implement these measures. In addition, they believed the NRC should clarify its intent regarding access control measure (e.g., control of shipment at

foreign port of entry). Staff intent in the draft was for licensees to confirm the identity of shippers and receivers of material. Staff identified other sections in the existing measures that would satisfy the intent of positive identity of persons involved in the transfer of material. Thus, the entire section Access Controls was removed.

Several fuel cycle licensees commented that the measures for Category III international shipments appear to exceed the licensee's authority, capability or control at shipping ports of export, ocean air transport, foreign ports and personnel involved at these locations. Licensees do not have the capability or authority to limit personnel access and badge all personnel who handle the shipment for export until the shipment is delivered to its final destination. As a result, staff clarified that the measures are applicable within the U.S. and edited them to underscore the domestic portion of the shipment is what is being addressed, not the entire transit.

Several fuel cycle licensees commented that the measures for transportation security of Category III heightened security appear to confuse the purpose of the section and that no corresponding measures exists in fixed site facilities with Category III material. As a result, staff revised those measures for transportation security of Category III material to only take certain actions when notified by the NRC of heightened threat conditions.

Several fuel cycle licensees commented that the Category III measures for Maintenance and Testing appears to be a new requirement. Staff determined these measures would not provide additional security. As a result, the entire section was removed for Category III transportation security.

Several fuel cycle licensees commented that the measures for the use of a corrective action program for Category III transport appeared to be a new requirement. Staff revised this section to indicate the measure will be a modification of the existing licensees programs in place.

Cost

Many stakeholders provided qualitative information regarding the cost or burden associated with either a set of physical protection measures or individual measures. Staff revised Section 8 to include this information. A few stakeholders provided more detailed cost information. This information is not captured in this regulatory basis but will be used by staff in its development of the Regulatory Analysis for the proposed rule.

8. Cost/Impact Considerations

This section discusses cost and other impacts for the proposed changes presented in Section 4, "Basis for Requested Changes." This section discusses potential impacts on three groups: (1) licensees, (2) the NRC, and (3) State, local, or Tribal Governments. Potential environmental impacts are also discussed. The analyses presented in this section are qualitative and based on staff's assessment and input from stakeholders. A more detailed cost/impact evaluation will be carried out as part of the Regulatory Analysis in the proposed rule phase.

8.1 Applicability

Fixed-Site Physical Protection - The revision of the fixed-site physical protection requirements would be intended for all current fuel cycle licensees, other facilities that use and possess SNM licensed under Part 70, and non-power reactors. The new safety/safeguards interface measures would be intended for all current non-power reactors, fuel cycle licensees, and other facilities licensed under Part 70 that subject to §70.60.

Transportation Physical Protection - The revision of the transportation physical protection requirements would be intended for all current fuel cycle licensees or applicants for such license under Part 70 and non-power reactors licensees.

8.2 Potential Licensee Impacts

General

As discussed further below, new fixed site and transportation security measures and the restructuring of the regulations will result in an increased burden to licensees. In addition to the burden associated with implementing these new measures, licensee would bear a burden associated with having to modify site security plans and implementing procedures to incorporate the new measures and the revised format of the proposed regulatory structure. Licensees would also need to raise awareness of these changes to their staffs. The impact of potential additional training measures would likely occur early because most of the effort would be in the development of the knowledge and applicability of the new measures and the structure of the measures. With an appropriately chosen periodicity for continuing training in this area, additional resources required for long-term training capacity for licensee training departments should be minimal.

The proposed fixed site and transportation physical protection measures are intended to be more performance-based and less prescriptive; therefore, licensees would be provided flexibility in tailoring the overall physical protection program for site-specific conditions. This should ultimately result in a positive impact for some licensees (e.g., reduced cost, a physical protection program that is adjusted to site and licensee specific conditions). In addition, the structure of the new measures was revised to add clarity that should reduce regulatory uncertainty and ultimately reduce the burden on licensees.

Given the improvements provided by considering material attractiveness, it is possible that some facilities (licensees with Category I material) might choose to modify their current fixed site physical protection programs to take advantage of changes in physical protection measures for material that is less attractive. Also fuel cycle facility and non-power reactor licensees might modify their plans to take advantage of changes in transportation security measures for material that is less attractive. For Category I – highly dilute materials, the transportation security requirements are significantly less than those for existing Category I material. For HUE non-power reactor fuel, the burden is expected to be small because the existing Category II fixed site and transportation security requirements are essentially the same as the Category II – moderately dilute measures and less than those proposed measures for Category II non-dilute material. In cases where licensees modify their current fixed site physical protection programs

to take advantage of changes in physical protection measures for material that is less attractive, licensees would be impacted by having to modify their security plans, implementing procedures, and physical protection equipment and barriers, but the overall burden could be reduced because lower cost would be incurred in providing less physical protection for less attractive material.

Based on comments and discussions provided during the September 24, 2014, public meeting, several licensees believe that the proposed approaches and changes to physical protection measures would result in an additional burden, with no measurable increase in safety or security. Stakeholders also commented that it was difficult at this stage of the rulemaking for them to identify a measurable increase in safety or security and to provide cost impacts because the measures were open to interpretation and detailed guidance was not provided. Staff recognizes that many of the measures were conceptual and open to interpretation. However staff expects that guidance development associated with the proposed rule will clarify the appropriate scope for these proposed requirements. As with any rulemaking process, stakeholders will see draft rule language as it develops and have the opportunity to comment on proposed rule language and guidance documents.

Fixed-Site Physical Protection

The NRC recognizes that existing facilities have physical protection programs that address the existing regulations and applicable portions of security orders or confirmatory action letters. It is expected that, for most existing licensees, the physical protection program activities currently undertaken would not significantly change as a result of the new regulation; and, therefore, the impact on most licensees will be small. The proposed changes for the existing fuel cycle facility licensees (with Category I and Category III material) do not involve changes to physical features (i.e., changes requiring construction of walls, barriers, guard posts, etc.) of the physical protection program. Similarly, the proposed changes for existing non-power reactors do not involve changes to the physical features of the physical protection program. Additional burden for both fuel cycle and non-power reactor licensees would be required to implement new features such as safety/safeguards interface, program review, Category III security plan measures. It is expected that burden for these new measures would be small.

The new safety/safeguards interface measures would apply to all categories of non-power reactors and applicable fuel cycle licensees. As with the current §73.58 interface requirement for reactors, it is expected that licensees would rely on, and take credit for, existing processes to the maximum extent practical. Examples might include reviews of process changes, procedure changes, and maintenance order review processes. If current work-management processes, configuration-control programs, and processes required by Part 70 Subpart H and the requirements of §50.59 adequately control facility activities to prevent adverse interactions between safety/safeguards, these processes should continue to be used. However, in complying with such a new measure, it might be necessary for these processes to be reviewed and revised to account for the potential for adverse safety/safeguards interactions. When changes are required, they might range from inclusion of each discipline in the approval process to simply raising the awareness of potential interactions. While each licensee would be responsible for implementing any changes to procedures and facility activities in response to the new measure, the maximum use of existing programs should lessen the associated cost and burden.

Several non-power reactor licensees noted that some of the new measures could inhibit research. They further noted that due to limited staffing and resources any changes would impact their programs. A non-power reactor licensee noted that while they currently meet the new proposed measures, the proposed measures are above current regulations. Thus, this situation could result in continual expense in maintaining systems and personnel that are currently voluntary. However the staff feels the proposed changes, which are consistent with activities that are already being done to meet the existing regulations and commitments in the confirmatory action letters, are needed to adequately protect the material.

For Category II (moderately dilute) material, non-power reactor licensees noted that a number of new measures could cause the facilities to incur additional costs. These include measures for random searches of facility users, badging, periodic patrols of outside areas, weekly testing of intrusion and search equipment, audit of the security plan by an outside auditor, and an annual security exercise. They also noted that the measure to establish and maintain a security organization designed, staffed, trained, qualified, and equipped including having individuals on-site 24/7, would be a very significant cost impact. As a result of these comments, changes were made to the proposed measures in Attachment 7. In some cases, previously proposed measures were deleted. In other cases, the proposed measure was made more performance-based. Staff believes the burden associated with these proposed measures outweighs the benefit of ensuring adequate protection of the material.

Several fuel cycle and non-power reactor licensees with Category III material noted that the new measures for a security plan would cause additional costs and could result in the need for additional security personnel and training. Staff did not change its proposed approach from the draft regulatory basis and believes that the benefit of having an NRC-approved security plan for the applicable SNM outweighs the increased burden. A fuel cycle facility licensee noted the additional burden associated with an access authorization program, controlling access control devices and escort communications. Staff believes that the benefit of the proposed measures for the applicable SNM outweighs the increased burden. For instance, a robust access authorization program will help to limit the risk of insiders aiding or accomplishing misuse of SNM for malevolent purposes. Also implementation experience has identified that the potential for theft or diversion and malevolent use of those materials warrant the submission and approval of a security plan.

Transportation Physical Protection

The most significant transportation security enhancements proposed in the regulatory basis apply to shipments of high-risk materials, including Category I non-dilute, Category I - moderately-dilute, and Category II non-dilute materials. Presently, NRC licensees are not responsible for shipping such materials because they are shipped by the DOE Office of Secure Transportation which is exempt from NRC transportation security measures. Therefore, staff expects that the associated resource and cost impacts on the current licensees will be minimal for these changes. In contrast, NRC licensees routinely ship SNM that would be considered Category I highly-dilute, Category II moderately-dilute, and Category III nuclear materials. The proposed security enhancements for these materials are less significant and primarily capture the existing security and operational practices. Staff expects that the associated resource and cost impact will be small.

Several fuel cycle facility licensees with Category III material noted the additional burden associated with new measures (i.e., searching conveyances prior to loading, positively identifying persons receiving custody prior to transferring custody, enhancing communications in route, program reviews and clarifying roles and responsibilities of individuals involved in transportation security). It is expected that the burden associated with implementing these new measures would be small. Staff believes that the benefit of proposed measures for the applicable SNM outweighs the increased burden. This is because NRC has not updated its transportation physical protection requirements to account for changes in the threat environment. This rulemaking also affords the opportunity to more closely align the NRC transportation security requirements and the requirements promulgated by other U.S. Government agencies, as well as the international recommendations of INFCIRC/225 Rev. 5 (IAEA, 2011), both of which considered the evolving threat. While protection of SNM in transit is a more challenging security task compared to ensuring security of SNM at fixed sites, these proposed measures incorporate risk insights to make transportation security more comparable to the level of protection of similar SNM at fixed sites.

8.3 Impact on the NRC

Proposed changes to fixed-site and transportation physical protection measures would require inspection resources from NRC regional staffs to support follow-on inspections of licensee programs. Also, as discussed in Section 10, “Guidance Documents,” supporting guidance would have to be evaluated and revised or developed for fixed site and transportation physical protection.

8.4 Impact on State, Local, or Tribal Governments

The proposed changes are unlikely to affect local, State or tribal government resources. Agreement State authorities would not be required to adopt a similar requirement for their licensees because quantities of SNM that could be regulated by an Agreement State do not require physical protection. As a result, State and local resource needs would be minimal.

8.5 Environmental Analysis

During the proposed rule phase, the proposed rule language will be analyzed for its potential effects on the environment. The NRC does not anticipate that a rule will have any negative impact on the environment.

9. NRC Strategic Plan

The NRC’s responsibility includes the regulation of commercial nuclear power plants; non-power reactors; nuclear fuel cycle facilities; medical, academic, and industrial uses of radioactive materials; the decommissioning of these facilities and sites; and the transport, storage, and disposal of radioactive materials and wastes. The NRC’s regulations are designed to protect the public and occupational workers from radiation hazards resulting from regulated activities and ensure the secure use of radioactive materials and SNM. Licensees are responsible for the safety and security of radioactive materials. To assist the NRC and its stakeholders in meeting

its responsibilities, the NRC prepares and updates a Strategic Plan (NRC, 2014b). This section explains how the recommended action will support the NRC's Strategic Plan goals, as well as their associated implementation strategies.

The NRC's strategic goals are:

- Safety: Ensure the safe use of radioactive materials.
- Security: Ensure the secure use of radioactive materials.

To achieve the security strategic goal, the NRC developed the following security-goal implementation strategies designed to avoid instances in which radioactive materials are used in a hostile manner.

1. Ensure the effectiveness of the regulatory framework using information gained from operating experience and assessments in response to technology advances and changes in the threat environment.

2. Maintain oversight of licensee performance to drive licensee compliance with NRC security requirements and license conditions.

3. Support U.S. security interests and nuclear nonproliferation policy objectives within the NRC statutory mandate through cooperation with domestic and international partners.

4. Ensure material control and accounting for special nuclear materials.

5. Protect critical digital assets.

6. Ensure timely distribution of security information to stakeholders and international partners.

7. Ensure that programs for handling and control of classified and Safeguards Information are effectively implemented at the NRC and licensed facilities.

The actions proposed in this regulatory basis support the NRC's Strategic Plan primarily in strategies 1 and 3.

Implementation strategy 1 is supported by updating SNM physical protection requirements for fixed sites and during transport to include generically applicable security requirements similar to those imposed by security orders that were based on updated threat intelligence, security assessments and sharing of information among domestic and international stakeholders. The proposed SNM physical protection measures also considered risk insights, implementation and oversight experience, and international guidance to make them more effective and realistic. For example, the LANL study considers a range of adversaries with differing capabilities to inform physical protection levels for different types, forms, and concentrations of SNM.

Using risk insights discussed in Section 3, "Regulatory Problem," to propose changes to the SNM physical protection at fixed sites and during transport supports implementation strategy 1. Many of the risk insights were based on National Laboratory studies to include material attractiveness, consideration of external radiation dose-rate threshold as a security feature and sabotage protection. The material attractiveness approach considers risk insights by more

realistically considering an adversary's ability to use SNM for malicious purposes and by informing the grading of physical protection measures. Implementing this approach will benefit licensees by "rightsizing" SNM physical protection requirements. The use of the current external radiation dose-rate threshold and current sabotage protections was determined to be inconsistent with the current risk posed by adversaries as discussed in Section 2, "Existing Regulatory Framework," and 3, "Regulatory Problem."

Implementation strategy 3 is supported by cooperating with domestic and international partners that occurred during the development of this regulatory basis. In addition to working and considering products of the National Laboratories, NRC also coordinated with the DOE and other Federal agencies on its material attractiveness approach. Staff also considered actions taken by other Federal agencies in protecting nuclear material and other critical infrastructure in determining if changes were required to NRC's existing SNM physical protection requirements. Moreover, as discussed in Section 7, "Stakeholder Interactions," the staff has conducted extensive stakeholder interactions including with international partners. Furthermore as part of this rulemaking effort, the staff reviewed and considered the International Atomic Energy Agency guidance identified in INFCIRC/225, revision 5 (IAEA, 2011).

Finally, the LANL studies will support the NRC's efforts (under implementation strategy 2) by updating its regulations for ensuring that security programs at licensees' sites continue to implement an effective security program for securing SNM in ways commensurate with the risk and attractiveness of each site's SNM inventory to an adversary for use in an IND. These actions will improve the effectiveness of NRC oversight programs and overall improve licensee's security programs.

10. Guidance Documents

The guidance development associated with this rulemaking will consist of new guidance, revising existing guidance, making conforming changes to existing guidance and rescinding guidance.

New guidance documents to be developed would include three RGs covering Category I, II, and III security plan format and content for fixed site physical protection and three RGs for Category I, II and III transportation physical protection requirements. These new RGs will include discussions of emerging technical areas including: material attractiveness; sabotage; and safety/safeguards interface, as applicable. A total of six Standard Review Plans would also need to be developed for Category I, II and III fixed site and transport security plan reviews. A new RG would be developed for physical protection at non-power reactors.

Existing guidance to be revised would include:

- NUREG-1964, "Access Control Systems" (2011), to have SNM monitor technology and Protected area/Material access area layout for Category I fixed sites described

- RG 5.80, "Pressure-Sensitive And Tamper-Indicating Device Seals for Material Control and Accounting of Special Nuclear Material" 2010, would be revised to include reference to Category II and III transport requirements and to align with the revised rule text

Conforming changes would be made to the following guidance documents:

- RG 5.44, “Perimeter Intrusion Detection Systems”
- RG 5.7 “Entry/Exit Control for Protected Areas, Vital Areas, and Material Access Areas”
- RG 5.12/DG 5027, "General use of Locks in the Protection and Control of Facilities and SNM”
- RG 5.27/ DG 5038, "Special Nuclear Material Doorway Monitors”

Rescinded guidance documents would include:

- RG 5.61, “Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites” (NRC, 1980b)
- RG 5.52, “Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material at Fixed Sites” (NRC, 1994)
- RG 5.55, “Standard Format and Content for Safeguards Contingency Plans” (NRC, 1978b)
- RG 5.59, “Standard Format and Content of a Licensee Physical Protection Plan for Special Nuclear Material of Moderate or Low Strategic Significance” (NRC, 1983),
- NUREG-1322, “Acceptance Criteria for the Evaluation of Category I Fuel Cycle Facility Physical Security Plans” (NRC, 1991)
- NUREG-1456, “An Alternative Format for Category I Fuel Cycle Facility Physical Protection Plans” (NRC, 1992)
- NUREG/CR-6667, “Standard Review Plan for Safeguards Contingency Response Plans for Category I Fuel Facilities” (NRC, 2000b),
- NUREG/CR-6668, “Standard Review Plan for Training and Qualifications Plans for Security Personnel at Category I Fuel Facilities” (NRC, 2000c)

Inspection procedures will also require revision. With respect to IMC 2600, approximately 30 inspection procedures would need to be updated for fixed site physical protection, and approximately 10 inspection procedures would need to be updated for transportation physical protection. With respect to IMC 2545, approximately 6 inspection procedures would need to be updated for non-power reactor physical protection.

All the revised and new guidance documents are expected to be issued in parallel with the proposed rule. Guidance that requires conforming changes would be updated as part of NRC’s periodic revision of existing guidance.

11. Resources

As discussed below, the rulemaking is being tracked by the Commission. As such, this rulemaking is included in the NRC budget process. Budgeted activities include developing the proposed and final rule packages, stakeholder interaction, guidance development, and development of inspection procedures.

12. Timing

The rulemaking included in this regulatory basis has been assigned a "high priority" and is being tracked by the Commission. The proposed rule and associated guidance are scheduled to be submitted to the Commission on or before September 2, 2016. The final rule is scheduled to be submitted to the Commission on or before March 15, 2018. No significant policy or legal issues were identified during the development of this regulatory basis that would need to be resolved before commencing rulemaking.

13. References

Atomic Energy Act (AEA), Pub. L. No. 83-703, 68 Stat. 919 (1954).

U.S. Atomic Energy Commission (AEC), "Special Nuclear Material," Final Rule, *Federal Register*, Vol. 21, No. 23, February 3, 1956, pp. 764–768 (21 FR 764).

AEC, "Physical Protection of Special Nuclear Material in Transit," Final Rule, *Federal Register*, Vol. 34, No. 67, April 9, 1969, pp. 6277–6279 (34 FR 6277).

AEC, "Physical Protection of Special Nuclear Material," Final Rule, *Federal Register*, Vol. 35, No. 76, April 18, 1970, pp. 6313–6315 (35 FR 6313).

AEC, "Physical Protection of Special Nuclear Material: Amended Requirements for Material in Transit," Final Rule, *Federal Register*, Vol. 38, No. 213, November 6, 1973, pp. 30533–30537 (38 FR 30533).

AEC, "Physical Protection of Plants and Materials," Final Rule, *Federal Register*, Vol. 38, No. 213, November 6, 1973, pp. 30537–30542 (38 FR 30537).

U.S. Department of Energy (DOE) (2000), "Manual for Control and Accountability of Nuclear Materials," M 474.1-1A, Washington, DC, November 22, 2000, available at https://www.directives.doe.gov/directives/0474.1-DManual-1a/view (accessed 04/12/14).

DOE (2005), "Nuclear Material Control and Accountability," M 470.4-6, Washington, DC, August 26, 2005, available at http://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/m4704-6c1.pdf (accessed 04/12/14).

DOE (2007), "Technical Review of the Department of Energy Graded Safeguards Table," Washington, DC, August 2007 (not publicly available).

Energy Policy Act (EPAct), Pub. L. No. 109-58, 119 Stat. 594 (2005).

Executive Office of the President, "Executive Order 13563: Improving Regulation and Regulatory Review," Final Rule, *Federal Register*, Vol. 76, No. 14, January 21, 2011, pp. 3821–3823 (76 FR 3821).

International Atomic Energy Agency (IAEA) (1975), "The Physical Protection of Nuclear Material," INFCIRC/225, September 1975, Vienna, Austria, available at http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc225.pdf (accessed 04/12/14).

IAEA (1980), "The Convention on the Physical Protection of Nuclear Material," INFCIRC/274, Revision 1, Vienna, Austria, May 1980, available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml (accessed 04/12/14).

IAEA (2010), "The Interface between Safety and Security at Nuclear Power Plants: A Report by the International Nuclear Safety Group," INSAG-24, Vienna, Austria, August 2010, available at http://www-pub.iaea.org/MTCD/publications/PDF/Pub1472_web.pdf (accessed 04/12/14).

IAEA (2011), "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," IAEA Nuclear Security Series No. 13, Vienna, Austria, January 2011, available at https://www.nss2014.com/sites/default/files/documents/infcirc225_rev5.pdf (accessed 04/12/14).

IAEA (2013), "International Physical Protection Advisory Service (IPPAS), International Atomic Energy Agency (IAEA), Mission Report: The United States of America, 30 September – 11 October 2013, Prepared for the Nuclear Regulatory Commission (NRC), The United States of America," Vienna, Austria, October 2013

Killar, Felix (2009), Nuclear Energy Institute, letter to Roy Zimmerman. Updating the MC&A and Security Requirements for Mixed Oxide Fuel, August 7, 2009, ADAMS Accession No. ML093030335.

U.S. Nuclear Regulatory Commission (NRC), "Part 70 – Special Nuclear Material," Final Rule, *Federal Register*, Vol. 21, February 3, 1956, pp. 764–768 (21 FR 764).

NRC, "Physical Protection of Special Nuclear Material In Transit," Final Rule, *Federal Register*, Vol. 34, No. 67, April 9, 1969, pp. 6277 - 6279 (34 FR 6277).

NRC, "Physical Protection of Special Nuclear Material," Final Rule, *Federal Register*, Vol. 35, No. 76, April 18, 1970, pp. 6313 - 6315 (35 FR 6313).

NRC, "Physical Protection of Plants and Materials: Performance Oriented Safeguards Requirements," Proposed Rule, *Federal Register*, Vol. 42, No. 128, July 5, 1977, pp. 34310–34321 (42 FR 34310).

NRC (1977), “NRC and International Physical Protection Standards,” SECY-77-79, February 11, 1977.

NRC, “Physical Protection of Plants and Materials,” Proposed Rule, *Federal Register*, Vol. 43, No. 154, August 9, 1978, pp. 35321–35337 (43 FR 35321).

NRC (1978a), “Physical Protection of Category II and III Material,” SECY-78-142, March 9, 1978, Agencywide Documents Access and Management System (ADAMS) Accession No. ML12235A605 (not publically available).

NRC (1978b), “Standard Format and Content of Safeguards Contingency Plans for Fuel Cycle Facilities,” Regulatory Guide (RG) 5.55, March 1978, ADAMS Accession No. ML003739256.

NRC (1978c), “Standard Format and Content of Safeguards Contingency Plans for Transportation,” RG 5.56, March 1978, ADAMS Accession No. ML003739236.

NRC, “Safeguard Requirements for Special Nuclear Material of Moderate and Low Strategic Significance,” Final Rule, *Federal Register*, Vol. 44, No. 143, July 24, 1979, pp. 43280–43285 (44 FR 43280).

NRC, “Physical Protection Upgrade Rule,” Final Rule, *Federal Register*, Vol. 44, No. 230, November 28, 1979, pp. 68184–68199 (44 FR 68184).

NRC (1980a), “Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material in Transit,” RG 5.60, April 1980, ADAMS Accession No. ML003739262.

NRC (1980b), “Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites,” RG 5.61, June 1980, ADAMS Accession No. ML003739270.

NRC (1982), “Low Enriched Uranium (LEU) Reform Amendments,” SECY-82-375, September 14, 1982, ADAMS Accession No. ML12241A642 (not publicly available).

NRC (1983), “Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance,” RG 5.59, Rev. 1, February 1983, ADAMS Accession No. ML100341301.

NRC, “Physical Protection Requirements for Nonpower Reactor Licensees Possessing Formula Quantities of Strategic Special Nuclear Material,” Proposed Rule, *Federal Register*, Vol. 48, No. 145, July 27, 1983, pp. 34056–34060 (48 FR 34056).

NRC (1984), “Low Enriched Uranium (LEU) Reform Amendments,” SECY-84-362, September 13, 1984, ADAMS Accession No. ML12243A723 (not publicly available).

NRC (1991), “Acceptance Criteria for the Evaluation of Category I Fuel Cycle Facility Physical Security Plans,” NUREG-1322, October 1991 (not publicly available).

NRC (1992), “An Alternative Format for Category I Fuel Cycle Facility Physical Protection Plans,” NUREG-1456, June 1992 (not publicly available).

NRC, “Physical Protection of Plants and Materials,” Proposed Rule, *Federal Register*, Vol. 58, No. 48, March 15, 1993, p. 13700 (58 FR 13700).

NRC (1994), “Standard Format and Content of a License Physical Protection Plan for Strategic Special Nuclear Material at Fixed Sites (Other than Nuclear Power Plants),” RG 5.52, Rev. 3, December 1994, ADAMS Accession No. ML003739235.

NRC, “Physical Protection for Spent Nuclear Fuel and High-Level Radioactive Waste,” Final Rule, *Federal Register*, Vol. 63, No. 94, May 15, 1998, pp. 26955–26963 (63 FR 26955).

NRC (2000a), “Risk-informed Regulation Implementation Plan,” SECY-00-0062, March 15, 2000, ADAMS Accession No. ML003691939.

NRC (2000b), “Standard Review Plan for Safeguards Contingency Response Plans for Category I Fuel Facilities,” NUREG/CR-6667, May 2000, ADAMS Accession No. ML003718179 (not publicly available).

NRC (2000c), “Standard Review Plan for Training and Qualifications Plans for Security Personnel at Category I Fuel Facilities,” NUREG/CR-6668, May 2000, ADAMS Accession No. ML003719803.

NRC (2004b), “Research and Test Reactor Inspection Program,” Inspection Manual Chapter (IMC) 2545, June 23, 2004, ADAMS Accession No. ML041810395.

NRC (2005), ‘‘Managing the Safety/Security Interface,’’ Information Notice 2005-33, December 30, 2005 (not publicly available).

NRC (2006a), “Schedules and Resources for Security Rulemakings,” SRM-COMSECY-05-0058, February 8, 2006, ADAMS Accession No. ML060390527 (not publicly available).

NRC, “Design-Basis Threat,” Final Rule, *Federal Register*, Vol. 72, No. 52, March 19, 2007, pp. 12705–12727 (72 FR 12705).

NRC (2008), “Technical Basis for Proposed Rulemaking Regarding Fingerprinting and Authorization for Unescorted Access to Radioactive Materials,” September 20, 2008, ADAMS Accession No. ML082270364 (not publicly available).

NRC, “Power Reactor Security Requirements,” Final Rule, *Federal Register*, Vol. 74, No. 58, March 27, 2009, pp. 13926–13993 (74 FR 13926).

NRC (2009), “Material Categorization and Future Fuel Cycle Facility Security-Related Rulemaking,” SECY-09-0123, September 4, 2009, ADAMS Accession No. ML12285A057.

NRC (2010), “Fuel Cycle Facility Operational Safety and Safeguards Inspection Program,” IMC 2600, January 27, 2010, ADAMS Accession No. ML093420698.

NRC (2012a), “Regulation of Chemical Security,” SRM-SECY-11-0108, February 15, 2012, ADAMS Accession No. ML120470207.

NRC (2012b), “The Nuclear Regulatory Commission Cyber Security Roadmap,” SECY-12-0088, June 25, 2012, ADAMS Accession No. ML12135A050.

NRC (2013a), “Protecting Our Nation,” NUREG/BR-0314, Rev. 3, October 2013, ADAMS Accession No. ML13270A213.

NRC (2013b), “Reprocessing Regulatory Framework – Status and Next Steps,” SRM-SECY-13-0093, November 4, 2013, ADAMS Accession No. ML11308A403.

NRC, “Amendments to Material Control and Accounting Regulations,” Proposed Rule, *Federal Register*, Vol. 78, No. 217, November 8, 2013, pp. 67225–67252 (78 FR 67225).

NRC (2014a), “Regulatory Basis Document – Draft for Public Comment: Rulemaking for Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation; Security Fatigue at Nuclear Facilities,” RIN number 3150-AJ41, May 2014, ADAMS Accession No. ML14113A468.

NRC, “Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation,” Draft regulatory basis; request for comment, *Federal Register*, Vol. 79, No. 117, June 18, 2014, pp. 34641–34642 (79 FR 34641).

NRC, “Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation,” Draft regulatory basis; extension of comment period, *Federal Register*, Vol. 79, No. 140, July 22, 2014, pp. 42474–42475 (79 FR 42474).

NRC (2014b), “Strategic Plan: Fiscal Years 20140–2018,” NUREG-1614, Vol. 6, September 5, 2014, ADAMS Accession No. ML14111241A517.

Oak Ridge National Laboratory (ORNL) (2005), “Radiation Effects on Personnel Performance Capability and a Summary of Dose Levels for Spent Research Reactor Fuels,” ORNL/TM-2005/261, Oak Ridge, TN, December 2005, available at http://web.ornl.gov/~webworks/cppr/y2007/rpt/124368.pdf (accessed 04/12/14).

Pietrangelo, Anthony (2013), Nuclear Energy Institute, letter to Michael Johnson and Michael Weber. Initial Industry Proposals to Address the Cumulative Impact of Regulatory Actions, April 16, 2013, ADAMS Accession No. ML13113A163 (publicly available)

Plain Writing Act: Federal Agency Requirements, Pub. L. No. 111-274, 124 Stat. 2861 (2010).

Radiation Source Protection and Security Task Force (RSPSTF), "The 2010 Radiation Source Protection and Security Task Force Report," August 11, 2010, ADAMS Accession No. ML102230141.

Schlueter, Janet (2013), Nuclear Energy Institute, letter to John Kinneman. Cumulative Impact of Regulation on Fuel Cycle Facilities – Input for Discussion at April 11, 2013 Public Meeting in Atlanta, Georgia, April 3, 2013, ADAMS Accession No. ML13107B383 (publicly available)

Sandia National Laboratories (SNL) (2009), "Estimate of Minimum Mass of Nuclides in RDD and RED Applications," SAND2009-8186, Albuquerque, NM, December 2009 (classified).

SNL (2013a), "Transport Security Regulations/Requirements Comparison: NRC Part 73 as Compared to DOE M 470.4B," SAND2013-4785P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013b), "Transport Security Regulations/Requirements Comparison: NRC Part 73 as Compared to DOE M 460.2-1A," SAND2013-4786P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013c), "Transport Security Regulations/Requirements Comparison – NRC Part 73 and INFCIRC/225/Rev. 5," SAND2013-4790P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013d), "Comparison of INFCIRC/225, Rev. 5 Transport Security Provisions with Similar Provisions in NRC Regulations: Category III (Low Strategic Significance) Only," SAND2013-4792P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013e), "Transport Security Regulations/Requirements Comparison: NRC Part 73 as compared to DOE M 470.4B," SAND2013-4792P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013f), "Transport Security Regulations/Requirements Comparison: NRC Part 73 as compared to DOE GSP," SAND2013-5027P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013g), "Transport Security Regulations/Requirements Comparison: NRC Part 73 and DOE M 473.3," SAND2013-5028P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013h), Sandia National Laboratories, "Comparison of INFCIRC/225, Rev. 5 Transport Security Provisions with Similar Provisions in NRC Regulations: Category I (Formula Quantity) Only," SAND2013-5029P, Albuquerque, NM, June 2013 (not publicly available).

SNL (2013i), Sandia National Laboratories, "Comparison of INFCIRC/225, Rev. 5 Transport Security Provisions with Similar Provisions in NRC Regulations: Category II (Moderate Strategic Significance) Only," SAND2013-5030P, Albuquerque, NM, June 2013 (not publicly available).

Sapountzis, Alexander P. (2014a), NRC, memorandum to William Gott, NRC, February 6, 2014, ADAMS Accession No. ML14055A273.

Sapountzis, Alexander P. (2014b), NRC, memorandum to William Gott, NRC, February 20, 2014, ADAMS Accession No. ML14072A438.

Sapountzis, Alexander P. (2014c), NRC, memorandum to William Gott, NRC, April 9, 2014, ADAMS Accession No. ML14107A102.

Sapountzis, Alexander P. (2014d), NRC, memorandum to William Gott, NRC, May 28, 2014, ADAMS Accession No. ML14155A069.

Sapountzis, Alexander P. (2014e), NRC, memorandum to William Gott, NRC, July 11, 2014, ADAMS Accession No. ML14192A255.

Sapountzis, Alexander P. (2014f), NRC, memorandum to William Gott, NRC, October 21, 2014, ADAMS Accession No. ML14292A044.

Sapountzis, Alexander P. (2014g), NRC, memorandum to William Gott, NRC, October 28, 2014, ADAMS Accession No. ML14300A003.

Virgilio, Martin J. (2002), NRC, letter to B. Marie Moore, Nuclear Fuel Services, Inc., August 21, 2002, ADAMS Accession No. ML022490244 (not publicly available).

Virgilio, Martin J. (2003), NRC, letter to Scott Wilkerson, Framatome Advanced Nuclear Power, Inc., February 6, 2003, ADAMS Accession No. ML030420134 (not publicly available).

ABBREVIATIONS AND ACRONYMS

AEA	Atomic Energy Act of 1954, as amended
AEC	Atomic Energy Commission
ASM	Additional Security Measure
CAL	Confirmatory Action Letter
CEA	Commissariat à l'énergie atomique et aux énergies alternatives (France)
CFR	*Code of Federal Regulations*
DBT	design-basis threat
DOE	U.S. Department of Energy
EPAct	Energy Policy Act of 2005
f.o.b.	free on board
FCIX	Fuel Cycle Information Exchange
FR	*Federal Register*
g/l	grams per liter
GPS	Global Positioning System
HEU	Highly Enriched Uranium
IAEA	International Atomic Energy Agency
ICM	Interim Compensatory Measures
IMC	Inspection Manual Chapter
IND	improvised nuclear device
INMM	Institute of Nuclear Materials Management
JNES	Japan Nuclear Energy Safety Organization
JNRA	Japanese Nuclear Regulation Authority
LANL	Los Alamos National Laboratory
LEU	Low-Enriched Uranium
LLEA	local law-enforcement agency
MAA	material access area
MAWH	maximum average work-hour [limit]
MC&A	material control and accounting
MEDDE	le ministère de l'Écologie, du Développement durable et de l'Énergie (France)
MoD	Ministry of Defence (UK)
MOX	mixed-oxide [fuel]
NEI	Nuclear Energy Institute
NNSA	National Nuclear Security Administration
NRC	U.S. Nuclear Regulatory Commission
NTSB	National Transportation Safety Board
OCNS	Office of Civil Nuclear Security (UK)
ONR	Office for Nuclear Regulation (UK)
ORNL	Oak Ridge National Laboratory
OST	Office of Secure Transportation
PA	protected area
Pu	plutonium
Pu-238	plutonium-238 [isotope]
Pu/Be	plutonium/beryllium
RDD	radiological dispersal device
RED	radiological exposure device
RG	Regulatory Guide

RQ	reportable quantities
RSPSTF	Radiation Source Protection and Security Task Force
SGDSN	Secrétariat général de la défense et de la sécurité nationale (France)
SNF	spent nuclear fuel
SNL	Sandia National Laboratory
SNM	special nuclear material
SRM	Staff Requirements Memorandum
U-233	uranium-233 [isotope]
U-235	uranium-235 [isotope]
WINS	World Institute for Nuclear Security
wt %	weight percent

Attachment 1 – Outreach Initiatives

Outreach Initiatives for the Regulatory Basis

Date	Outreach Item
05/13/2010	Meeting: Nuclear Energy Institute (NEI)/Nuclear Regulatory Commission (NRC) to Discuss Reprocessing Regulatory Framework
09/09/2010	Reprocessing Public Workshop - Rockville, MD
10/19/2010	Reprocessing Public Workshop - Albuquerque, NM
03/24/2011	Launch NRC Web Page
05/24/2011	Briefing for representatives of the Department of Energy (DOE)/National Nuclear Security Administration (NNSA) Office of Defense Nuclear Security and Office of Nuclear Safeguards and Security, the Office of Health, Safety and Security, and the Department of State
05/25/2011	Briefing for representatives of the Australian Safeguards and Non-Proliferation Office
06/06/2011	Public Meeting on the Fuel Cycle Oversight Process - Rockville, MD
06/07/2011	Briefing for representatives of the Spanish Nuclear Safety Council
06/08/2011	Fuel Cycle Information Exchange Public Meeting - Rockville, MD
06/22/2011	Reprocessing Public Workshop - Augusta, GA
07/13/2011	Briefing of representatives of NNSA/Office of Secure Transportation (OST).
07/21/2011	Briefing for representatives of the Australian Safeguards and Non-Proliferation Office and UK Office of Civil Nuclear Security
8/25-26/2011	Briefing for Canadian Nuclear Safety Commission (Ottawa, Canada).
09/06/2011	Briefing for Spain representatives (Madrid, Spain).
09/09/2011	Briefing for UK OCNS and MOD representatives (Oxford, UK).
11/09/2011	Briefing for French representatives (Paris/Fontenay Aux Roses, France).
11/11/2011	Briefing for UK OCNS and MOD representatives (London/Oxford, UK).
04/26/2012	Briefing for Argentina Nuclear Regulatory Authority (Buenos Aires, Argentina).
06/14/2012	Fuel Cycle Information Exchange (FCIX) Public Meeting - Rockville, MD
08/01/2012	Updated NRC Web Page
12/01/2012	Security Regulators Conference-Rockville, MD
12/3-5/2012	Discussions with representatives of France, UK and Russia at International Security Regulators Conference

1/15-16/2013	Presentations to MEDDE, SGDSN, CEA of the government of France.
01/17/2013	Presentation to DECC, MOD, ONR, Cabinet Office of the UK.
04/02/2013	Presentation at INMM Reducing Risk Workshop in Washington, DC
4/8-12/2013	Discussion with representatives of UK, Netherlands, Japan and Russia at NUSAT CM in Vienna, Austria
04/10/2013	Presentation to NEI Fuel Cycle Meeting in Atlanta, GA
6/4-6/2013	Meetings with MEDDE and SGDSN of the government of France in Albuquerque, NM
06/10/2013	CER Meeting in Rockville, MD
06/13/2013	FCIX in Rockville, MD
7/1-5/2013	Presentation at IAEA Security Conference in Vienna
7/15-18/2013	Presentations at INMM Annual Meeting in Palm Desert, CA
07/23/2013	Meetings with CEA, SGDSN of the government of France and the MOD, ONR, Cabinet Office of the UK in Washington, D.C.
07/24/2013	Updated NRC Web Page
09/19/2013	Presentation at Ohio State University Nuclear Forum, Columbus, OH
09/24/2013	Presentation to National Organization of Test, Research, and Training Reactors in St. Louis, MO.
10/01/2013	CER Meeting in Rockville, MD
12/16/2013	Discussion with representatives of Japan (JNES and JNRA) in Rockville, MD
01/14/2014	CER Meeting in Rockville, MD
01/27-28/2014	Discussions with representatives of France and UK.
1/30-31/2014	Workshop Sponsored by Princeton Univ. and Union Concerned Scientist, Washington D.C.
01/30/2014	Updated NRC Web Page
02/06/2014	Public Meeting-Webinar in Rockville, MD
2/11-12/14	Panel Discussion at INMM Workshop on Risk Informing Security, Stone Mountain, GA
02/18/2014	Updated NRC Web Page
02/18/2014	Discussions with the National Organization of Test, Research, and Training Reactors Executive Committee in Rockville, MD.
02/20/2014	Public Meeting-Webinar in Rockville, MD
02/21/2014	Discussions with the National Institute of Standards and Technology in Gaithersburg, MD.
03/05/2014	CER Meeting in Rockville, MD

03/13/2014	INMM Meeting at George Washington University, Washington D.C.
03/18/2014	Discussions with representatives of France (WINS), a non-government agency
03/19/2014	Discussions with representatives of India (BARC)
04/07/2014	Updated NRC Web Page
04/09/2014	Public Meeting-Webinar in Rockville, MD
05/20/2014	Discussions with the National Organization of Test, Research, and Training Reactors Executive Committee in Rockville, MD.
05/23/2014	Updated NRC Web Page
05/28/2014	Public Meeting-Webinar in Rockville, MD
06/02/2014	Briefing for UK and France representatives.
06/09/2014	CER Meeting in Rockville, MD
06/12/2014	Public Meeting on the draft Regulatory Basis in Rockville, MD.
7/20-24/2014	INMM 55th Annual Meeting in Atlanta, GA
08/06/2014	Presentation to National Organization of Test, Research, and Training Reactors in Portland, OR.
09/17/2014	Public Meeting on the draft Regulatory Basis in Rockville, MD, primarily with Research and Test Reactor licensees.
09/22/2014	CER Meeting in Rockville, MD
09/22-23/2014	Discussions with Research and Test Reactor licensees in MA.
09/24/2014	Public Meeting on the draft Regulatory Basis in Rockville, MD.
10/27/2014	Discussions with Pennsylvania State University in University Park, PA.

Attachment 2 – List of Comments Received on the Draft Regulatory Basis

1. Thomas H. Newton, Jr., Ph.D., Director of Reactor Operations - MIT Nuclear Reactor Laboratory, Request for Extension of Public Comment Period on 10 CFR Part 26/73, June 24, 2014. (ADAMS Accession No. ML14175A947)

2. Janet R. Schlueter, Senior Director, Fuel and Materials Safety - Nuclear Energy Institute, Request for Extension of Public Comment Period on 10 CFR Part 26/73, Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation, , June 20, 2014. (ADAMS Accession No. ML14174A421)

3. Daniel J. Cronin, Licensing Engineer - University of Florida Training Reactor, Requesting an Additional Public Meeting on the Draft Regulatory Basis, June 23, 2014. (ADAMS Accession No. ML14181A871)

4. R. Vann Bynum, Ph.D., Chief Operating Officer - SHINE Medical Technologies, Inc., Requesting Extension of Public Comment Period, July 1, 2014. (ADAMS Accession No. ML14183B587)

5. Melinda Krahenbuhl, Chair, TRTR - Reed College, Requesting Extension of Public Comment Period, June 26, 2014. (ADAMS Accession No. ML14195A498)

6. Mark A. Trump, Associate Director for Operations - Pennsylvania State University, Requesting Extension of Public Comment Period, June 30, 2014. (ADAMS Accession No. ML14195A501)

7. Jeffrey Leavey, Radiation Safety Officer - Pennsylvania State University, Requesting Extension of Public Comment Period, July 8, 2014. (ADAMS Accession No. ML14205A706)

8. Melinda Krahenbuhl, Chair - National Organization of Test, Research, and Training Reactors, Requesting an Extension of the Public Comment Period, June 26, 2014. (ADAMS Accession No. ML14206B154)

9. Jacob McCandless, Regarding Enhanced Security at Fuel Cycle Facilities, August 1, 2014. (ADAMS Accession No. ML14218A574)

10. Cameron Goodwin, Director - Rhode Island Nuclear Science Center, Regarding Enhanced Security at Fuel Cycle Facilities, October 3, 2014. (ADAMS Accession No. ML14276A653)

11. James Costedio, Licensing Manager - SHINE Medical Technologies, Inc., Regarding Physical Protection of Special Nuclear Material at NRC-licensed facilities and in Transit, October 10, 2014. (ADAMS Accession No. ML14287A578)

12. Thomas H. Newton, Jr., Ph.D., Director of Reactor Operations - MIT Nuclear Reactor Laboratory, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation; and Security Force Fatigue at Nuclear Facilities, October 10, 2014. (ADAMS Accession No. ML14288A565)

13. Thomas Newton and Edward Lau, Co-Chairs - National Organization of Test, Research and Training Reactors, Regarding Enhanced Security at Fuel Cycle Facilities, October 10, 2014. (ADAMS Accession No. ML14288A576)

14. Kelly D. Trice, President and COO - CB&I AREVA MOX Service, LLC, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation, October 15, 2014. (ADAMS Accession No. ML14289A606)

15. Ralph A. Butler, Director - University of Missouri Research Reactor Center, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportations; Security Force Fatigue at Nuclear Facilities, October 16, 2014. (ADAMS Accession No. ML14289A612)

16. Mark A. Trump, Associate Director for Operations - Penn State Radioactive Science and Engineering Center, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportations, October 17, 2014. (ADAMS Accession No. ML14290A400)

17. Steve Reese, Director - Oregon State University Radiation Center, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportations; Security Force Fatigue at Nuclear Facilities, October 16, 2014. (ADAMS Accession No. ML14290A479)

18. Nancy Blair Parr, Manager, Licensing - Westinghouse Columbia Fuel Fabrication Facility, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportations; Security Force Fatigue at Nuclear Facilities, October 17, 2014. (ADAMS Accession No. ML14290A591)

19. Daniel J. Cronin, Licensing Engineer - University of Florida Training Reactor, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportations; Security Force Fatigue at Nuclear Facilities, October 17, 2014. (ADAMS Accession No. ML14290A593)

20. Edwin Lyman, Senior Scientist, Global Security Program - Union of Concerned Scientists, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation, October 17, 2014. (ADAMS Accession No. ML14293A326)

21. Andrew Kauffman, Associate Director - Ohio State University Research Reactor, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation, October 17, 2014. (ADAMS Accession No. ML14293A610)

22. Matthew Bunn, Professor of Practice - Harvard Kennedy School, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation, October 18, 2014. (ADAMS Accession No. ML14293A636)

23. Janet R. Schlueter, Senior Director, Fuel and Materials Safety - Nuclear Energy Institute, Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation, October 17, 2014. (ADAMS Accession No. ML14294A445)

24. Scott Murray on behalf of Global Nuclear Fuel-Americas (GNF-A) Regarding Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportation.), October 24, 2014. (ADAMS Accession No. ML14297A527)

25. T.J. Tate, Manager, Environmental, Health, Safety & Licensing - AREVA, Inc., Regarding Enhanced Security at Fuel Cycle Facilities, Special Nuclear Material Transportation, October 17, 2014. (ADAMS Accession No. ML14300A252)

Attachment 3 – Category I: Fixed Site Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. [73.20(a)][12]

The physical protection program should protect against the design basis threats of theft or diversion and radiological sabotage as stated in § 73.1 and should be designed to prevent the removal of SNM and other unauthorized activities involving SNM. [73.1]

The physical protection program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness.

In addition to these fixed-site requirements, the NRC may require, depending on the individual facility and site conditions, alternate or additional measures deemed necessary to protect against theft or diversion of Category I SNM. [73.46(a)]

Licensees should ensure that the design of the physical protection program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities. [1]

Licensees should analyze and identify site-specific conditions that may affect the specific measures needed to implement the requirements of this section and should account for these conditions in the design of the physical protection program. [1] The design of the physical protection program should be informed by an insider risk analysis. [1]

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures. [1] [73.46(b)(1)]

Licensees should establish, maintain, and implement a performance evaluation program in accordance with Part 73, Appendix B to demonstrate and assess the effectiveness of armed responders and armed security officers to implement the protective strategy. [73.46(b)(9)]

Licensees should establish, maintain, and implement an access authorization program in accordance with 10 CFR Part 11 and insider mitigation program and should describe the program in the Physical Security Plan. [Part 11] [2]

---

[12] Where applicable, a reference to existing regulations is provided at the end of the proposed measures. In addition, proposed measures developed with consideration of risk insights are noted with a “1” and proposed measures developed with consideration of security orders are noted with a “2”.

Licensee should establish, maintain, and implement an insider mitigation program and should describe the program in the Physical Security Plan. The insider mitigation program should monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected, vital or material access area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent theft or diversion or radiological sabotage. [2]

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program. [1] [73.46(g)(5)]

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions. [1]

Security Plans

Licensees should develop, maintain and implement a Physical Security Plan that describes how they will meet the performance objective and physical protection requirements. [73.20(c)]

Licensees should develop, maintain and follow a Training and Qualification Plan that describes how they will meet the criteria in Part 73, Appendix B. [73.46(b)(4)]

Licensees should develop, maintain and implement a Safeguards Contingency Plan that describes how they will meet the criteria in Part 73, Appendix C. [73.46(h)(1)]

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans. [73.46(b)(3)]

Security Organization

Licensees should establish and maintain a security organization that is designed, staffed, trained, qualified and equipped to implement its physical protection program. [73.46(b)(1)]

The security organization should follow a management system to oversee the physical protection program including having at least one member (onsite and available at all times) to direct activities. [73.46(b)(2&3)]

Members of the security organization should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties. [73.46(b)(1 & 4)]

A member of the security organization may not be assigned to or have direct operational control over more than one of the redundant elements of the physical protection system, if such assignment or control could result in the loss of effectiveness of the physical protection program. [73.46(b)(5)]

Physical Barriers

Performance capabilities

Licensees should identify and analyze site-specific conditions to determine the specific use, type, function and placement of physical barriers needed to satisfy the general performance objective and requirements. The physical barriers should control access into facility areas and be designed to protect against the theft or diversion design basis threat and the radiological design basis threat, account for site specific conditions, perform their required functions, and provide deterrence, delay or support access control. [2] [73.46(c)(1)]

Openings in any barrier should be secured and monitored to prevent exploitation of the opening consistent with the function of the barrier.

Bullet resistant barriers

The central alarm station, secondary alarm station and the location within which the last access control function for access to the protected area is performed, should be bullet-resisting. [73.46(e)(5), 73.46(d)(4)]

Owner controlled areas

Licensees should establish and maintain physical barriers in the owner controlled area as needed to satisfy the general performance objective and requirements. [2]

Isolation zone

An isolation zone should be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone should be designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier. Obstructions that could prevent the licensee's capability to meet the observation and assessment requirements of this section should be located outside of the isolation zone. [73.46(c)(3)]

The isolation zone should be monitored with intrusion detection equipment designed and capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier.

The isolation zone should be monitored with assessment equipment designed to provide real-time and play- back/recorded video images of the detected activities before and after each alarm annunciation.

Protected area

The protected area perimeter should be protected by physical barriers that are designed and constructed to limit access into the protected area, channel personnel, vehicles and materials to designated access control portals, and be separate from any other physical barrier. [73.46(c)(1 & 2)]

Penetrations through the protected area barrier should be secured and monitored to prevent and detect exploitation of the openings. All emergency exits in the protected area barrier should be alarmed and secured by locking devices. Where walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary.

Vital area

Vital equipment should only be located within vital areas or material access areas, within a protected area so that access to vital equipment requires passage through at least two physical barriers. More than one vital area may be located within a single protected area. [73.46(c)(1)]

Licensees should protect all vital area access portals and vital area emergency exits with intrusion detection equipment and locking devices that allow rapid egress during an emergency. [73.46(e)(2)]

Unoccupied vital areas should be locked and alarmed. [73.46(e)(3)]

At a minimum, the following should be considered vital areas: (1) central alarm station; and (2) secondary alarm station. [73.46(e)(5)]

At a minimum, the following should be located within a vital area: (1) the secondary power supply systems for alarm annunciation equipment; and (2) the secondary power supply systems for non-portable communications equipment.

Material access area

Material access area barriers should be designed and constructed to satisfy the general performance objective and requirements including to delay any unauthorized penetration attempts by persons, vehicles or materials sufficient to assist detection and permit a response that will prevent the penetration. [73.45(b)(1)]

Material access area barriers should limit access into the material access area, channel personnel, vehicles and materials to designated access control portals, and be separate from any other physical barrier. [73.45(b)(1)]

Penetrations through the material access area barrier should be secured and monitored to prevent and detect exploitation of the openings. All emergency exits in the material access area barrier should be alarmed and secured by locking devices. [73.46(e)(2)]

High enriched uranium, plutonium or uranium-233 should be used, processed and stored within a material access area. Except, high enriched uranium in containers larger than 30 gallons in the form of small pieces, cuttings, chips or solutions with uranium-235 concentrations less than 0.25 grams per liter may be stored in a controlled access area inside a protected area. More than one material access area may be located within a single protected area. [73.46(c)(1), 73.46(c)(5), 73.46(c)(6)]

Areas used for preparing high enriched uranium, plutonium or uranium-233 for shipment and areas used for packaging and screening waste should be located in a controlled access areas and should be separated from processing and storage areas. [73.46(d)(12)]

Category I quantities of high enriched uranium, plutonium or uranium-233 should be stored in tamper-indicating containers. Intermediate storage of high enriched uranium, plutonium or uranium-233 during processing should be kept in locked compartments or locked process equipment, except when personally attended. [73.46(c)(5)]

Vaults

Category I quantities of high enriched uranium, plutonium or uranium-233 (other than alloys, fuel elements or assemblies) should be stored in a vault when not undergoing processing , except when personally attended. [73.46(c)(5), 1]

Vaults should be capable of preventing entry to stored high enriched uranium, plutonium or uranium-233 by a single act, except when the single act would destroy the barrier and render the Category I SNM incapable of being removed, and should provide sufficient delay to prevent removal of high enriched uranium, plutonium or uranium-233prior to arrival of response personnel. [73.46(c)(5)]

Vault doors should be kept closed and locked when authorized activities are not taking place. [2]

Vehicle control measures

Licensees should design, construct, install and maintain a vehicle barrier system to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems. [2]

The operation of vehicle barriers should be periodically checked. A secondary power source or a means of mechanical or manual operation should be provided to ensure that active barriers can be placed in the denial position. Vehicle barriers should be periodically surveilled and observed to detect indications of tampering and degradation. [2]

Where rail access is provided into the protected area, additional measures including installing a train derailer, removing a section of track, or restricting access to railroad sidings, should be provided. [2]

Licensees should identify areas from which a waterborne vehicle should be restricted and install buoys, markers or other equipment to restrict access. Water approaches should be periodically surveilled and observed. [2]

<u>Insider mitigation program [2]</u>

Licensees should establish, maintain, and implement an insider mitigation program and should describe the program in the Physical Security Plan.

The insider mitigation program should monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected, material access or vital area, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent the theft or diversion and radiological sabotage. The insider mitigation program and associated measures may be graded to require more robust measures for material access areas and vital areas.

The insider mitigation program should contain elements from (1) the access authorization program described in Part 11; (2) the fitness-for-duty program described in Part 26; and (3) the physical protection program; and (4) Part 74, checks and balances sufficient to detect

falsification and reports that could conceal diversion. In meeting these requirements, the insider mitigation program should consider and be harmonized with programs required by other federal agencies (i.e., the Department of Energy).

Behavioral observation program

Access authorization programs should include a behavioral observation program that is designed to detect behaviors or activities that may constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit theft, diversion or radiological sabotage.

Licensees should ensure that individuals granted unescorted access to the protected areas, material access areas or vital areas are subject to behavioral observation applicable to that security area.

Each person subject to the behavior observation program should be responsible for communicating to the licensee observed behaviors of individuals subject to behavioral observation program. Such behaviors include any behavior of individuals that may adversely affect the safety or security of the facility or that may constitute an unreasonable risk to the public health and safety or the common defense and security, including a potential threat to commit theft, diversion or radiological sabotage.

Licensees should ensure that individuals who are subject to the behavioral observation program successfully complete initial behavioral observation training and requalification behavior observation training. The training program should be graded based on the duties and responsibilities of the individual and the security areas they have unescorted access.

For initial behavioral observation training, managers and supervisors should demonstrate successful completion by passing a comprehensive examination that addresses the knowledge and abilities necessary to detect behavior or activities that have the potential to constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit theft, diversion or radiological sabotage. Remedial training and re-testing are required for managers and supervisors who fail to satisfactorily complete the examination.

Individuals should complete refresher training on a nominal 12-month frequency, or more frequently where the need is indicated. Individuals may take and pass a comprehensive examination that meets the above requirements in lieu of completing annual refresher training.

Initial and refresher training may be delivered using a variety of media, including, but not limited to, classroom lectures, required reading, video, or computer-based training systems. Licensees should monitor the completion of training.

Individuals who are subject to an access authorization program should at a minimum, report any concerns arising from behavioral observation, including, but not limited to, concerns related to any questionable behavior patterns or activities of others to his or her supervisor, or other management personnel designated in their site procedures. Licensees should reassess the reported individual's unescorted access or unescorted access authorization status. Licensees should determine the elements of the reassessment based on the accumulated information of the individual. If licensees have a reason to believe that the reported individual's

trustworthiness or reliability is questionable, licensees should either administratively withdraw or terminate the individual's unescorted access or unescorted access authorization while completing the reevaluation or investigation.

Self-reporting of legal actions

Any individual who has applied for unescorted access or unescorted access authorization or is maintaining unescorted access or unescorted access authorization should promptly report to his or her supervisor, or other management personnel designated in site procedures, any legal action(s) taken by a law enforcement authority or court of law to which the individual has been subject that could result in incarceration or a court order or that requires a court appearance, including but not limited to an arrest, an indictment, the filing of charges, or a conviction, but excluding minor civil actions or misdemeanors such as parking violations or speeding tickets. On the day that the report is received, licensees should evaluate the circumstances related to the reported legal action(s) and re-determine the reported individual's unescorted access or unescorted access authorization status.

Licensees should inform the individual of this obligation, in writing, prior to granting unescorted access or certifying unescorted access authorization.

Access Controls

Performance capabilities

Licensees should control personnel, vehicle and material access at each access control point consistent with the function of each barrier as needed to satisfy the general performance objective and requirements. [73.46(d)(2, 3, 4, 8 & 9), 73.45(b & f)]

Access control portals should be located outside or concurrent with the physical barrier through which it controls access and should be equipped with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function.

Licensees should provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment.

Licensees should establish, implement, and maintain a list of individuals who are authorized to have unescorted access to vital and material access areas. The list should include only those individuals who have a continued need for access to those areas in order to perform their duties and responsibilities. The list should be approved by a cognizant security manager, and updated and re-approved periodically. [2]

Individuals responsible for performing the last access control function at the protected area access control portal should be isolated and located in a bullet-resisting structure to assure the ability to respond or summon assistance. [73.46(d)(4)]

Licensees should limit unescorted access to the protected, vital and material access areas to only individuals who require unescorted access to perform assigned duties and responsibilities. [73.46(d)(2)]

Access control systems should be designed to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions. Licensees should implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment. [2]

Protected areas

Licensees should, before granting access into protected areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements.

Licensees should exercise control over all vehicles inside the protected area to ensure that they are used only by authorized individuals and for authorized purposes. When not in use the vehicles keys should be removed or the vehicle should be otherwise disabled. [73.46(d)(8)]

Vehicles transporting hazardous materials inside the protected area should be escorted by a member of the security organization. [73.46(d)(8)]

Vital Areas

Licensees should control access into vital areas consistent with access authorization lists. [73.46(d)(2)]

In response to a site-specific credible threat or other credible information, implement a two-person (line-of-sight) rule for all personnel in vital areas so that no one individual is permitted access to a vital area. This requirement does not apply to central or secondary alarm stations.

Material access areas

Licensees should control access into material access areas to only those personnel, vehicles and material which require access to high enriched uranium, plutonium or uranium-233; to equipment used in the processing, use, or storage of high enriched uranium, plutonium or uranium-233; or to perform necessary maintenance. [73.46(d)(2 & 9)]

At least two armed guards should be posted at material access area portals when in use. [73.46(d)(2 & 9)]

Licensees should, before granting access into material access areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements. [73.46(d)(9)]

Access to material access areas should include at least two authorized individuals. [73.46(d)(2)]

Access control devices

Licensees should control all keys, locks, combination, passwords and related access control devices used to control access to controlled, protected, vital and material access areas, and security systems to reduce the probability of compromise. [73.46(d)(14)]

Access control devices should only be issued to individuals with unescorted access who require those devices to perform official duties and responsibilities. Licensees should maintain a list of individuals which have been issued access control devices and implement a process to account for access control devices at least annually. Upon less than favorable termination of employment, access control devices that were issued or accessed by that employee should be changed. [73.46(d)(14)]

Licensees should implement compensatory measures upon discovery that any access control device may have been compromised. Compensatory measures should remain in effect until the compromise is corrected. [73.46(g)(5)]

Licensees should implement a numbered photo identification badge for all individuals authorized unescorted access to controlled access, protected, vital and material access areas. Badges should be clearly displayed by all individuals inside controlled access, protected, vital and material access areas. [73.46(d)(1)] Badging should include special coding to identify which areas individuals have access. [73.46(d)(2)]

Licensees should maintain a record, to include name and areas to which unescorted access is granted, of all individuals issued photo identification. [2]

Visitors

Licensees may permit escorted access to controlled access, protected, vital and material access areas to individuals who have not been granted unescorted access. Licensees should develop and implement procedures for processing, escorting and controlling visitors which include confirmation of identity, listing of visitors, issuance of a visitor badge, establishing escort ratios, monitoring visitor activities, and escorting visitors at all times. [73.46(d)(13)]

Licensees should ensure that all escorts are trained to perform escort duties, have unescorted access to areas in which they perform escort duties, and have a means of timely communication with security personnel to summon assistance if needed.

Individuals not employed by licensees who require frequent or extended unescorted access to controlled access, protected, vital or material access areas to perform duties and responsibilities required by licensees should satisfy the access authorization requirements and be issued a non-employee photo identification badge. [73.46)d)(1)]

<u>Search Programs</u>

Performance capabilities

Search programs should detect, deter and prevent the introduction of firearms, explosives, incendiary devices or other items which could be used to aid in the theft or diversion of SNM. Search programs should also detect, deter and prevent the removal or diversion of SNM. Only authorized and confirmed forms and amounts of high enriched uranium, plutonium or uranium-233 should be removed from material access areas. [2]

Federal, State and local law enforcement personnel on official duty and U.S. Department of Energy couriers engaged in transporting SNM and their vehicles are excepted from search requirements. [73.46(d)(4)]

Owner controlled area

Where physical barriers are provided in the owner controlled area, licensees should implement search procedures for access control points in the barrier. Licensees should develop and implement procedures for vehicle search at vehicle access portals to include searching the cab, engine compartment, under carriage and cargo areas, as appropriate. Vehicle searches should be performed by at least two (2) trained and equipped security personnel, one of which should be armed. The armed individual should be positioned to observe the search process and provide immediate response. [2]

Vehicle searches should be accomplished through the use of equipment capable of detecting explosives, incendiary devices, or other items which could be used to commit aid in theft or diversion or radiological sabotage, or through visual and physical searches, or both, to ensure that all items are identified before granting access. Vehicle access control points should be equipped with video surveillance equipment that is monitored by an individual capable of initiating a response. [2]

Protected area

Licensees should search all personnel, vehicles and materials requesting access to protected areas. [73.46(d)(4, 5 & 6)]

Search for firearms, explosives, incendiary devices or other contraband should be accomplished through the use of equipment capable of detecting those items, or through visual and physical search or both, to ensure that all items are clearly identified before granting access to protected areas. When search equipment is out of service, is not operating satisfactorily, or cannot be used effectively, a visual and physical search should be conducted. [2] [73.46(d)(4, 5 &7)]

When an attempt to introduce prohibited items has occurred or is suspected, licensees should implement actions to ensure that suspect individuals, vehicles and materials are denied access and should perform a visual and physical search to determine the absence or existence of a threat. [73.46(d)(4)]

Licensees should conduct personnel searches for SNM and metal shielding upon exit from the protected area. Metal searches may be random.

Licensees should develop and implement procedures for vehicle search at vehicle access portals to include searching the cab, engine compartment, under carriage and cargo areas. [73.46(d)(7)]

Licensees may develop and implement exceptions to protected area search requirements for safety or operational reasons provided that the general performance objective and requirements are satisfied through specific security measures which could include positively controlling materials, storing in locked areas, escorting by an armed member of the security organization, verify material at off-loading.

Material access area

Licensees should search all personnel, vehicles and materials requesting access to material access areas.

Licensees should, for ingress and egress to a material access area, preclude commingling of searched and unsearched personnel. [1]

Entry searches for firearms, explosives, incendiary devices or other contraband should be accomplished through the use of equipment capable of detecting those items, or through visual and physical search or both, to ensure that all items are clearly identified before granting access to material access areas. [73.46(d)(9)] When search equipment is out of service, is not operating satisfactorily, or cannot be used effectively, a visual and physical search should be conducted.

When an attempt to introduce prohibited items has occurred or is suspected, licensees should implement actions to ensure that suspect individuals, vehicles and materials are denied access and should perform a visual and physical search to determine the absence or existence of a threat.

Licensees should develop and implement procedures for vehicle entry searches at vehicle access portals to include searching the cab, engine compartment, under carriage and cargo areas.

Licensees should perform two separate searches of all personnel exiting a material access area, one for concealed high enriched uranium, plutonium or uranium-233 and one for metal or other shielding material. For areas containing alloyed or encapsulated high enriched uranium, plutonium or uranium-233, the second search may be conducted in a random manner. [73.46(d)(9), 73.46(h)(8)]

Vehicles, materials and packages exiting the material access area should be searched for concealed high enriched uranium, plutonium or uranium-233 by at least two security officers. [73.46(d)(9)]

High enriched uranium, plutonium or uranium-233 being prepared for shipment offsite should be packed and placed in sealed containers in the presence of two individuals working as a team to verify and certify the contents of each shipping container. [73.46(d)(11)]

Containers of contaminated wastes should be scanned and tamper sealed by at least two individuals working as a team. [73.46(d)(10)]

<u>Detection and Assessment Systems</u>

Performance capabilities

Licensees should establish and maintain intrusion detection and assessment systems that satisfy the general performance objective and requirements and provide, at all times, the capability to detect and assess unauthorized activities, persons or materials and facilitate the protective strategy. [73.46(e)(1), 73.46(h)(6)]

Intrusion detection and assessment systems should be designed to provide visual and audible annunciation of alarms, provide visual display to facilitate assessment, ensure alarm and annunciation of the type and location of the alarm, provide automatic indication when the alarm system or component fails or is operating on backup power, ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device without the knowledge and concurrence of the other alarm station operator and support the initiation of a timely response. [73.46(e)(7), 73.46(h)(7)]

Transmission lines should be tamper indicating and self-checking. [73.46(e)(7)]

Intrusion detection and assessment equipment at the protected and material access area perimeters should remain operable from an uninterruptable power supply in the event of the loss of normal power. [73.46(e)(6), 2]

All emergency exits in protected and material access areas should be locked and alarmed both locally and at alarm stations. [73.46(e)(2)]

All unoccupied material access areas should be locked and protected with intrusion detection equipment or at least two armed security officers. [73.46(e)(3)]

Alarms occurring within unoccupied vaults or unoccupied material access areas containing unalloyed or unencapsulated high enriched uranium, plutonium or uranium-233 should be assessed by at least two security personnel using closed caption television or other remote means. [73.46(h)(8)]

Alarm Stations

Intrusion detection equipment should annunciate and video assessment equipment should display concurrently in at least two continuously staffed on-site alarm stations (i.e., central alarm station and secondary alarm station). [73.46(e)(5)]

Alarm stations should be designed and equipped to ensure that a single act cannot disable both alarm stations. Alarm station walls, doors, ceiling, floor and windows should be bullet resisting. [73.55(e)(5)] Licensees should ensure the survivability of at least one alarm station to maintain the ability to perform its functions including detect and assess alarms, initiate and coordinate adequate response to alarms, summon off-site assistance, and provide command and control. [73.46(e)(5)] [2]

The central alarm station should be located in a protected area and should not be visible from the perimeter of the protected area. [73.46(e)(5)]

Alarm stations should be continuously staffed with at least one trained and qualified alarm station operator who should not be assigned other duties or responsibilities which would interfere with the operator's ability to execute the functions of the alarm station. [73.46(e)(5)]

Alarm station operators should assess and initiate response to all alarms and other events, as appropriate, in accordance with security plans and implementing procedures. Alarm station operators should be knowledgeable of the final disposition of and maintain a record of all alarms.

Surveillance, observation and monitoring

The physical protection program should include surveillance, observation and monitoring as needed to satisfy the general performance objective and requirements, identify indications of tampering or otherwise implement the protective strategy. Surveillance should ensure that only authorized activities occur within the material access area including authorized placement and movement of high enriched uranium, plutonium or uranium-233.

Licensees should provide continuous surveillance, observation and monitoring of the owner controlled area to detect and deter intruders, and ensure the integrity of physical barriers or other components and functions of physical protection program. This may be performed by security personnel during continuous patrols, through video technology or a combination of both. [2]

Unattended openings that intersect a security boundary should be protected by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation. [1]

All exterior areas within the protected area should be monitored or periodically checked to detect and deter unauthorized personnel, vehicles and materials. [73.46(e)(8)]

Armed security patrols should periodically check external areas of the protected areas to include physical barriers and material access portals. [73.46(e)(8), 2] Armed security patrols should periodically inspect material access areas to include physical barriers. [2]

Methods to observe individuals within material access areas should be provided and used on a continuing basis to ensure that high enriched uranium, plutonium or uranium-233 is not moved to unauthorized locations or in an unauthorized manner. [73.46(e)(9)]

Vaults and process areas that contain high enriched uranium, plutonium or uranium-233 should be surveilled with close circuit television monitored in alarm stations. [73.46(e)(3)]

Security personnel should be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Upon detection of tampering, licensees should initiate response in accordance with security plans and implementing procedures.

Illumination

Licensees should ensure that all areas of the facility are provided with illumination necessary to satisfy the general performance objective and requirements or otherwise implement the protective strategy.

Licensees should provide a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zone and appropriate exterior areas within the protected area. [73.46(c)(4)] Alternatively, licensees may augment the facility illumination system by means of low-light technology.

Communication

Performance capabilities

Licensees should establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations. [2] [73.46(f)(1)]

Alarm station operators should be capable of calling for assistance in accordance with security plans and implementing procedures. [73.46(f)(2)]

All on-duty security force personnel should be capable of maintaining continuous communication with an individual in each alarm station, and vehicle escorts should maintain continuous communication with security personnel. All personnel escorts should maintain timely communication with security personnel. [73.46(f)(1)]

Alarm stations, in addition to telephone service, should be capable of radio or microwave transmitted two-way voice communication either directly or through an intermediary to local law enforcement. [73.46(f)(2)]

Non-portable communications equipment should remain operable from independent power sources in the event of loss of normal power. [73.46(f)(3), 2]

Licensees should identify site areas where communication could be interrupted or cannot be maintained and should establish alternative communication measures for those areas.

Response

Performance capabilities

Licensees should establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats up to and including the design basis threats for theft or diversion and radiological sabotage to prevent the removal of SNM and other unauthorized activities involving SNM. [73.46(h)(1)]

Licensees should ensure that all firearms, ammunition and equipment necessary to implement security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

Licensees should train each armed member of the security organization to prevent or impede acts of theft or diversion and radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law. [73.46(h)(5)]

Licensees should provide armed response personnel consisting of tactical response team personnel which may be augmented by armed security officers to carry out armed response duties specified in the protective strategy. [73.46(h)(3)]

Tactical Responders

Licensees should determine the minimum number of tactical response team members to satisfy the general performance objectives and requirements and implement the protective strategy. This number should be documented in security plans and should not be less than eight. [73.46(h)(3), 2]

Tactical response team members should be available at all times inside the protected area and may not be assigned other duties or responsibilities that could interrupt with their assigned response duties.

Armed security officers

Armed security officers, designated to strengthen response capabilities, should be onsite and available at all times to carry out their assigned response duties.

The minimum number of armed security officers designated to strengthen onsite response capabilities should be documented in security plans. [73.46(h)(3)]

Protective Strategy

Licensees should establish, maintain and implement a written protective strategy in accordance with the requirements in Appendix C of Part 73. [73.46(h)(1)]

Upon receipt of an alarm or other indication of a threat, licensees should determine the existence and level of the threat in accordance with pre-established assessment methodologies, initiate response actions to interrupt and neutralize the threat in accordance with the requirements in Part 73, Appendix C, and notify law enforcement agencies in accordance with site procedures. [73.46(h)(4)]

Law enforcement liaison

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. [73.46(h)(2), 2]

Heightened security

Licensees should establish, maintain and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. [1,2]

Licensees should ensure that the specific protective measures and actions identified for each threat level are consistent with security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat. [2]

Security Program Review

Licensees should review each element of the physical security program at least every 12 months based upon site-specific analysis, assessments or other performance indicators. The reviews should be conducted by individuals independent of the physical security program. [73.46(g)(6)]

Reviews should be conducted within 12 months following initial implementation or a change in personnel, procedures, equipment or facilities that potentially could adversely affect security.

Reviews should include an audit of the effectiveness of the physical security program, security plans, implementing procedures, safety/safeguards interface activities, testing and maintenance program, and response commitments by local, State and Federal law enforcement authorities. [73.46(g)(6)]

The results and recommendations of these reviews, management findings regarding the program, and any actions taken as a result of previous program reviews should be documented in a report to facility and corporate management. These reports should be maintained in an auditable form and available for inspection. [73.46(g)(6)]

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptable power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions. [73.46(g), 73.46(g)(4), 73.46(g)(5)]

The maintenance and testing program should be described in security plans.

During installation and construction of physical protection related components, licensees should assure that they comply with their respective design criteria and performance specifications. [73.46(g)(1)]

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented.

Licensees should test each intrusion alarm for operability at the beginning and end of any period that it is used or, for continuous operation, at least once every seven days. [73.46(g)(3)]

Intrusion detection and access control equipment should be performance tested in accordance with security plans and implementing procedures.

Onsite communication equipment should be tested for operability not less frequently than once at the beginning of each security personnel work shift. [73.46(g)(3)] Communication systems between alarm stations and local law enforcement agencies, including backup communication, should be tested for operability at least once per day. [73.46(g)(3)]

Search equipment should be tested for operability at least once each day and tested for performance at least during each seven day period.

Security equipment or systems should be testing in accordance with the site maintenance, testing and calibration procedures before being place in service (pre-operational), or before being placed back in service after each repair or inoperable state. [73.46(g)(5), 73.46(g)(2)] Repairs and maintenance should be performed by at least two individuals. [73.46(g)(5)]

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the physical security program. [73.46(g)(5)]

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in security plans and should not be used in lieu of performing timely maintenance.

Suspension of security measures

Licensees may suspend implementation of affected requirements under the following conditions:

(1) when suspension of security measures is immediately needed to protect the public health and safety and no action consistent with license conditions can provide adequate or equivalent protection is immediately apparent.

(2) during severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions can provide adequate or equivalent protection.

Suspended security measures should be reinstated as soon as conditions permit.

The suspension of security measures should be reported and documented in accordance with the provisions of § 73.71.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the onsite physical protection program, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Review and audit reports should be maintained and available for inspection, for a period of three (3) years.

Alternative measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 4 – Category I – Moderately Dilute: Fixed Site Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The physical protection program should be designed to immediately detect attempts to remove SNM and provide sufficient delay through the use of barriers and/or armed responders to allow local law enforcement agencies to promptly recovery SNM.

The physical protection program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness.

Licensees should ensure that the design of the physical protection program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

In addition to these fixed-site requirements, the NRC may require, depending on the individual facility and site conditions, alternate or additional measures deemed necessary to protect against theft or diversion of Category I - moderately dilute SNM.

Licensees should analyze and identify site-specific conditions that may affect the specific measures needed to implement the requirements of this section and should account for these conditions in the design of the physical protection program.

Upon the request of an authorized representative of the NRC, licensees should demonstrate the ability to meet NRC requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

Licensees should establish, maintain, and implement an access authorization program in accordance with Part 11 and should describe the program in the Physical Security Plan.

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions.

Security Plans

Licensees should develop, maintain and implement a Physical Security Plan that describes how they will meet the performance objective and physical protection requirements.
Licensees should develop, maintain and follow a Training and Qualification Plan that describes how they will meet the criteria in Part 73, Appendix B, except for tactical response training and qualification.

Licensees should develop, maintain and implement a Safeguards Contingency Plan that describes how they will meet the criteria in Part 73, Appendix C.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans. .

Security Organization

Licensees should establish and maintain a security organization that is designed, staffed, trained, qualified and equipped to implement its physical protection program.

The security organization should follow a management system to oversee the physical protection program including having at least one member (onsite and available at all times) to direct activities.

Members of the security organization should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties.

A member of the security organization may not be assigned to or have direct operational control over more than one of the redundant elements of the physical protection system, if such assignment or control could result in the loss of effectiveness of the physical protection program.

Physical Barriers

Performance capabilities

Licensees should identify and analyze site-specific conditions to determine the specific use, type, function and placement of physical barriers needed to satisfy the general performance objective and requirements. The physical barriers should control access into facility areas, account for site specific conditions, perform their required functions, and provide deterrence, delay or support access control.

Category I - moderately dilute SNM should be used, processed and stored within a controlled access area that is located within a protected area.

Openings in any barrier should be secured and monitored to prevent exploitation of the opening consistent with the function of the barrier.

Bullet resistant barriers

The central alarm station should be bullet-resisting.

Isolation zone

An isolation zone should be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone should be designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier.

Obstructions that could prevent the licensee's capability to meet the observation and assessment requirements of this section should be located outside of the isolation zone.

The isolation zone should be monitored with intrusion detection equipment designed and capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier.

The isolation zone should be monitored with assessment equipment designed to provide real-time and play- back/recorded video images of the detected activities before and after each alarm annunciation.

Protected area

The protected area perimeter should be protected by physical barriers that are designed and constructed to limit access into the protected area, channel personnel, vehicles and materials to designated access control portals, and be separate from any other physical barrier.

Penetrations through the protected area barrier should be secured and monitored to prevent and detect exploitation of the openings. All emergency exits in the protected area barrier should be alarmed and secured by locking devices. Where walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary.

All exterior areas within the protected area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Controlled access area

The controlled access area perimeter should be protected by a physical barrier that is designed and constructed to limit access into the controlled access area, and channel personnel, vehicles and materials to designated access control portals.

Other than fuel elements or fuel assemblies, Category I moderately dilute SNM should be stored in tamper-indicating containers in a vault-type room, unless the material is being processed or personally attended. Intermediate storage of Category I - moderately dilute SNM during processing should be kept in locked compartments or locked process equipment, except when personally attended.

The vault-type room should be equipped with an intrusion detection capability.

Penetrations through the controlled access area barrier should be secured and monitored to prevent and detect exploitation of the openings.

All exterior areas within the controlled access area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Vehicle control measures

Licensees should design, construct, install and maintain a vehicle barrier system to include passive and active barriers, to prevent unauthorized access of vehicles into the protected area.

The operation of vehicle barriers should be periodically checked. A secondary power source or a means of mechanical or manual operation should be provided to ensure that active barriers can be placed in the denial position. Vehicle barriers should be periodically surveilled and observed to detect indications of tampering and degradation.

Where rail access is provided into the protected area, additional measures including installing a train derailer, removing a section of track, or restricting access to railroad sidings, should be provided.

Licensees should identify areas from which a waterborne vehicle should be restricted and install buoys, markers or other equipment to restrict access. Water approaches should be periodically surveilled and observed.

Access Controls

Performance capabilities

Licensees should control personnel, vehicle and material access at each access control point consistent with the function of each barrier as needed to satisfy the general performance objective and requirements.

Access control portals should be located outside or concurrent with the physical barrier through which it controls access and should be equipped with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function.

Licensees should provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment.

Licensees should establish, implement, and maintain a list of individuals who are authorized to have unescorted access to protected areas and controlled access areas. The list should include only those individuals who have a continued need for access to those areas in order to perform their duties and responsibilities. The list should be approved by a cognizant security manager, and updated and re-approved periodically.

Individuals responsible for performing the last access control function at protected area access control portals should be isolated to assure the ability to respond or summon assistance.

Licensees should limit unescorted access to the protected and controlled access areas to only individuals who require unescorted access to perform assigned duties and responsibilities.

Access control systems should be designed to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions. Licensees should implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

Protected areas

Licensees should, before granting access into protected areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements.

Licensees should exercise control over all vehicles inside the protected area to ensure that they are used only by authorized individuals and for authorized purposes. When not in use the vehicles keys should be removed or the vehicle should be otherwise disabled.

Vehicles transporting hazardous materials inside the protected area should be escorted by a member of the security organization.

Controlled access areas

Licensees should, before granting access into control access areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements.

Licensees should exercise control over all vehicles inside the controlled access area to ensure that they are used only by authorized individuals and for authorized purposes.

Access control devices

Licensees should control all keys, locks, combination, passwords and related access control devices used to control access to protected areas and security systems to reduce the probability of compromise.

Access control devices should only be issued to individuals with unescorted access who require those devices to perform official duties and responsibilities. Licensees should maintain a list of individuals which have been issued access control devices and implement a process to account for access control devices at least annually. Upon less than favorable termination of employment, access control devices that were issued or accessed by that employee should be changed.

Licensees should implement compensatory measures upon discovery that any access control device may have been compromised. Compensatory measures should remain in effect until the potential compromise is corrected.

Licensees should implement a numbered photo identification badge program for all individuals authorized unescorted access to protected areas. Badges should be clearly displayed by all individuals inside protected areas.

Licensees should maintain a record, to include name and areas to which unescorted access is granted, of all individuals issued photo identification badge.

Visitors

Licensees may permit escorted access to protected areas to individuals who have not been granted unescorted access. Licensees should develop and implement procedures for processing, escorting and controlling visitors which include confirmation of identity, listing of visitors, issuance of a visitor badge, establishing escort ratios, monitoring visitor activities, and escorting visitors at all times.

Licensees should ensure that all escorts are trained to perform escort duties, have unescorted access to areas in which they perform escort duties, and have a means of timely communication with security personnel to summon assistance if needed.

Individuals not employed by licensees who require frequent or extended unescorted access to protected areas to perform duties and responsibilities required by licensees should satisfy the access authorization requirements and be issued a non-employee photo identification badge.

Search Programs

Performance capabilities

Search programs should detect, deter and prevent the introduction of firearms, explosives, incendiary devices or other items which could be used to aid in the theft or diversion of SNM. Search programs should also detect, deter and prevent the removal or diversion of SNM.

Licensees should search all personnel, vehicles and materials requesting access to protected areas.

Federal, State and local law enforcement personnel on official duty and U.S. Department of Energy couriers engaged in transporting SNM and their vehicles are excepted from search requirements.

Search for firearms, explosives, incendiary devices or other contraband should be accomplished through the use of equipment capable of detecting those items, or through visual and physical search or both, to ensure that all items are clearly identified before granting access to protected areas. When search equipment is out of service, is not operating satisfactorily, or cannot be used effectively, a visual and physical search should be conducted.

When an attempt to introduce prohibited items has occurred or is suspected, licensees should implement actions to ensure that suspect individuals, vehicles and materials are denied access and should perform a visual and physical search to determine the absence or existence of a threat.

Licensees should develop and implement procedures for vehicle search at vehicle access portals to include searching the cab, engine compartment, under carriage and cargo areas.

Licensees should search personnel, vehicles and packages leaving the controlled access area and protected area for unauthorized or concealed SNM, and for metal or other shielding material.

Licensees may develop and implement exceptions to protected area search requirements for safety or operational reasons provided that the general performance objective and requirements are satisfied through specific security measures which could include positively controlling materials, storing in locked areas, escorting by an armed member of the security organization, and verify material at off-loading.

Detection and Assessment Systems

Performance capabilities

Licensees should establish and maintain intrusion detection and assessment systems that satisfy the general performance objective and requirements and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the protective strategy.

Intrusion detection and assessment systems should be designed to provide visual and audible annunciation of alarms, provide visual display to facilitate assessment, ensure alarm and annunciation of the type and location of the alarm, provide automatic indication when the alarm system or component fails or is operating on backup power, and support the initiation of a timely response.

Transmission lines should be tamper indicating and self-checking.

Intrusion detection and assessment equipment at the protected area perimeter and vault-type room(s) should remain operable from an uninterruptable power supply in the event of the loss of normal power.

Alarm Stations

Intrusion detection equipment should annunciate and video assessment equipment should display concurrently in at least one continuously staffed on-site alarm stations (i.e., central alarm station). A secondary alarm station, which may be located off-site, should be capable of periodically verifying the status of the central alarm station, verifying that the central alarm station has resolved alarms and summoning off-site assistance, if needed.

The central alarm station should be designed and equipped to ensure that a single act cannot disable the alarm station. The central alarm station wall, doors, ceiling, floor and windows should be bullet resisting. Licensees should ensure the survivability of the central alarm station to maintain the ability to perform its functions including detect and assess alarms, initiate and coordinate adequate response to alarms, summon off-site assistance, and provide command and control.

The central alarm station should be located in a protected area and should not be visible from the perimeter of the protected area.

Alarm stations should be continuously staffed with at least one trained and qualified alarm station operator who should not be assigned other duties or responsibilities which would interfere with the operator's ability to execute the functions of the alarm station.

Alarm station operators should assess and initiate response to all alarms and other events, as appropriate, in accordance with security plans and implementing procedures. Alarm station operators should maintain a record of all alarms.

Surveillance, observation and monitoring

The physical protection program should include surveillance, observation and monitoring as needed to satisfy the general performance objective and requirements, identify indications of tampering or otherwise implement the protective strategy.

Unattended openings that intersect a security boundary should be protected by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation.

Armed security patrols should periodically check external areas of the protected areas to include physical barriers.

Security personnel should be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Upon detection of tampering, licensees should initiate response in accordance with security plans and implementing procedures.

Illumination

Licensees should ensure that all areas of the facility are provided with illumination necessary to satisfy the general performance objective and requirements or otherwise implement the protective strategy.

Licensees should provide a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zone and appropriate exterior areas within the protected area. Alternatively, licensees may augment the facility illumination system by means of low-light technology.

Communication

Licensees should establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

Alarm station operators should be capable of calling for assistance in accordance with security plans and implementing procedures.

All on-duty security force personnel should be capable of maintaining continuous communication with an individual in the central alarm station, and vehicle escorts should maintain continuous communication with security personnel. All personnel escorts should maintain timely communication with security personnel.

Alarm stations should be capable of two-way voice communication either directly or through an intermediary to local law enforcement using two independent means using different technologies.

Non-portable communications equipment should remain operable from independent power sources in the event of loss of normal power.

Licensees should identify site areas where communication could be interrupted or cannot be maintained and should establish alternative communication measures for those areas.

Response

Performance capabilities

Licensees should establish and maintain, at all times, properly trained, qualified and equipped personnel capable of interrupting unauthorized activities until local law enforcement arrives and to allow local law enforcement agencies to promptly recover SNM.

Licensees should ensure that all firearms, ammunition and equipment necessary to implement security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

Licensees should train each armed member of the security organization to interrupt unauthorized activities by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law.

Licensees should provide armed response personnel to carry out armed response duties specified in the protective strategy.

Armed security officers

Armed security officers should be onsite and available at all times to carry out their assigned response duties.

The minimum number of armed security officers should be documented in security plans.

Protective Strategy

Licensees should establish, maintain and implement a written protective strategy in accordance with the requirements in Part 73, Appendix C.

Upon receipt of an alarm or other indication of a threat, licensees should determine the existence and level of the threat in accordance with pre-established assessment methodologies, initiate response actions to immediately detect attempts to remove of SNM and provide sufficient delay through the use of barriers and/or armed responders to allow local law enforcement agencies to promptly recovery SNM in accordance with the requirements in Part 73, Appendix C, notify law enforcement agencies in accordance with site procedures.

Law enforcement liaison

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. To the extent practicable, licensees should conduct annual local law enforcement site familiarization activities to include a review of the protective strategy and on-site and off-site response procedures, and joint response exercises.

Heightened security

Licensees should establish, maintain and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

Licensees should ensure that the specific protective measures and actions identified for each threat level are consistent with the site's security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat.

Security Program Review

Licensees should conduct an exercise at least every 12 months to test the performance and effective implementation of its protective strategy and physical security procedures.

Licensees should review each element of the physical security program at least every 24 months based upon site-specific analysis, assessments or other performance indicators. The reviews should be conducted by individuals independent of the physical security program.

Reviews should be conducted within 12 months following initial implementation or a change in personnel, procedures, equipment or facilities that potentially could adversely affect security.

Reviews should include an audit of the effectiveness of the physical security program, security plans, implementing procedures, safety/safeguards interface activities, the testing and maintenance program, and response commitments by local, State and Federal law enforcement authorities.

The results and recommendations of these reviews, management findings regarding the program and any actions taken as a result of previous program reviews should be documented in a report to facility and corporate management. These reports should be maintained in an auditable form and available for inspection.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptable power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

The maintenance and testing program should be described in security plans.

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented.

Licensees should test each intrusion alarm for operability at the beginning and end of any period that it is used or, for continuous operation, at least once every seven days.

Intrusion detection and access control equipment should be performance tested in accordance with security plans and implementing procedures.

Onsite communication equipment should be tested for operability not less frequently than once at the beginning of each security personnel work shift. Communication systems between alarm stations and local law enforcement agencies, including backup communication, should be tested for operability at least once per day.

Search equipment should be tested for operability at least once each day and tested for performance at least during each seven day period.

Security equipment or systems should be testing in accordance with the site maintenance, testing and calibration procedures before being placed in service (pre-operational), or before being placed back in service after each repair or inoperable state.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the physical security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in security plans and should not be used in lieu of performing timely maintenance.

Suspension of security measures

Licensees may suspend implementation of affected requirements under the following conditions:

(1) when suspension of security measures is immediately needed to protect the public health and safety and no action consistent with license conditions can provide adequate or equivalent protection is immediately apparent.

(2) during severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions can provide adequate or equivalent protection.

Suspended security measures should be reinstated as soon as conditions permit.

The suspension of security measures should be reported and documented in accordance with the provisions of §73.71.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the onsite physical protection program, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Review and audit reports should be maintained and available for inspection, for a period of three (3) years.

Alternative measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 5 – Category I – Highly Dilute: Fixed Site Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The physical protection program should be designed to timely detect attempts to remove SNM and notify LLEA to recovery the SNM.

Licensees should analyze and identify site-specific conditions that may affect the specific measures needed to implement the requirements of this section and should account for these conditions in the design of the physical protection program.

In addition to these fixed-site requirements, the NRC may require, depending on the individual facility and site conditions, alternate or additional measures deemed necessary to protect against theft or diversion of Category I – highly dilute SNM.

Licensees should establish, maintain, and implement an access authorization program in accordance with 10 CFR Part 11 and should describe the program in the Physical Security Plan.

Licensee should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions.

Security Plans

Licensees should develop, maintain and implement a Physical Security Plan and implementing procedures that describes how they will meet the performance objective and physical protection requirements.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans.

Security Organization

Licensees should establish and maintain a security organization that is designed, staffed, trained, qualified and equipped to implement its physical protection program.

The security organization should follow a management system to oversee the physical protection program including having at least one member (onsite and available at all times) to direct activities and request off-site assistance.

Members of the security organization should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties. If members of the security organization are armed, the security plan should describe the training, qualification and requalification program.

Physical Barriers

Performance capabilities

Licensees should identify and analyze site-specific conditions to determine the specific use, type, function and placement of physical barriers needed to satisfy the general performance objective and requirements. The physical barriers should control access into facility areas, account for site specific conditions, perform their required functions, and provide deterrence, delay or support access control.

Controlled access area

The controlled access area perimeter should be protected by a physical barrier that is designed and constructed to limit access into the controlled access area, and channel personnel, vehicles and materials to designated access control portals.

Penetrations through the controlled access area barrier should be secured and monitored to prevent and detect exploitation of the openings.

All exterior areas within the controlled access area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Category I – highly dilute SNM should be used, processed and stored within a controlled access area.

Access Controls

Performance capabilities

Licensees should control personnel, vehicle and material access at each access control point consistent with the function of each barrier as needed to satisfy the general performance objective and requirements.

Access control portals should be located outside or concurrent with the physical barrier through which it controls access and should be equipped with locking devices, and surveillance equipment consistent with the intended function.

Licensees should provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment.

Individuals responsible for performing the last access control function at each access control portals should be isolated to assure the ability to respond or summon assistance.

Licensees should limit unescorted access to the controlled access area to only individuals who require unescorted access to perform assigned duties and responsibilities.

Access control systems should be designed to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions. Licensees should implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

Controlled access areas

Licensees should, before granting access into controlled access areas, confirm the identity of individuals; and verify the authorization for access of individuals, vehicles, and materials.

Licensees should exercise control over all vehicles inside the controlled access area to ensure that they are used only by authorized individuals and for authorized purposes.

Access control devices

Licensees should control all keys, locks, combination, passwords and related access control devices used to control access to controlled access areas and security systems to reduce the probability of compromise.

Access control devices should only be issued to individuals with unescorted access who require those devices to perform official duties and responsibilities. Licensees should maintain a list of individuals which have been issued access control devices and implement a process to account for access control devices at least annually. Upon less than favorable termination of employment, access control devices that were issued or accessed by that employee should be changed.

Licensees should implement compensatory measures upon discovery that any access control device may have been compromised. Compensatory measures should remain in effect until the compromise is corrected.

Licensees should implement a numbered photo identification badge program for all individuals authorized unescorted access to controlled access areas. Badges should be clearly displayed by all individuals inside controlled access areas.

Licensees should maintain a record, to include name and areas to which unescorted access is granted, of all individuals issued photo identification.

Visitors

Licensees may permit escorted access to controlled access areas to individuals who have not been granted unescorted access. Licensees should develop and implement procedures for processing, escorting and controlling visitors which include confirmation of identity, listing of visitors, issuance of a visitor badge, establishing escort ratios, monitoring visitor activities, and escorting visitors at all times.

Licensees should ensure that all escorts are trained to perform escort duties, have unescorted access to areas in which they perform escort duties, and have a means of timely communication with security personnel to summon assistance if needed.

Individuals not employed by licensees who require frequent or extended unescorted access to controlled access areas to perform duties and responsibilities required by licensees should satisfy the access authorization requirements and be issued a non-employee photo identification badge.

Detection and Assessment Systems

Performance capabilities

Licensees should establish and maintain intrusion detection and assessment systems that satisfy the general performance objective and requirements and provide the capability to detect and assess unauthorized persons and facilitate the protective strategy.

The control access area barrier should either:

(1) be monitored with an intrusion detection equipment

Intrusion detection systems should be designed to provide visual and audible annunciation of alarms, ensure alarm and annunciation of the type and location of the alarm, provide automatic indication when the alarm system or component fails or is operating on backup power and support the initiation of a timely response. Assessment of intrusion detection alarms should be performed by a member of the security organization.

or

(2) by periodic patrols to detect unauthorized penetrations or activities.

Security patrols should periodically check external areas of the controlled access areas to include physical barriers and access portals.

The physical protection program should include surveillance, observation and monitoring as needed to satisfy the general performance objective and requirements, or identify indications of tampering.

Security personnel should be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Upon detection of tampering, licensees should initiate response in accordance with security plans and implementing procedures.

Communication

Licensees should establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

A designated member of the security organization should be capable of calling for assistance in accordance with security plans and implementing procedures. Communication should be by two-way voice communication either directly or through an intermediary to local law enforcement using two independent means using different technologies.

All on-duty security force personnel should be capable of maintaining continuous communication with the individual responsible for requesting assistance. All personnel escorts should maintain timely communication with security personnel.

Non-portable communications equipment should remain operable from independent power sources in the event of loss of normal power.

Licensees should identify site areas where communication could be interrupted or cannot be maintained and should establish alternative communication measures for those areas.

Response

Licensees should ensure that a member of the security organization or offsite response force responds to all unauthorized penetrations or activities in accordance with security plans and response procedures.

Law enforcement liaison

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. To the extent practicable, licensees should conduct annual local law enforcement site familiarization activities to include a review of the protective strategy and on-site and off-site response procedures, and joint response exercises.

Heightened security

Licensees should establish, maintain and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

Licensees should ensure that the specific protective measures and actions identified for each threat level are consistent with security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat.

Security Program Review

Licensees should review each element of the physical security program at least every 24 months based upon site-specific analysis, assessments or other performance indicators. The reviews should be conducted by individuals independent of the physical security program.

Reviews should be conducted within 12 months following initial implementation or a change in personnel, procedures, equipment or facilities that potentially could adversely affect security.

Reviews should include an audit of the effectiveness of the physical security program, security plans, implementing procedures, safety/safeguards interface activities, and response commitments by local, State and Federal law enforcement authorities.

The results and recommendations of these reviews, management findings regarding the program and any actions taken as a result of previous program reviews should be documented in a report to facility and corporate management. These reports should be maintained in an auditable form and available for inspection.

Maintenance and Testing

Performance capabilities

For any security systems and equipment, licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

The maintenance and testing program should be described in security plans.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the physical security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in security plans and should not be used in lieu of performing timely maintenance.

Suspension of security measures

Licensees may suspend implementation of affected requirements under the following conditions:

> (1) when suspension of security measures is immediately needed to protect the public health and safety and no action consistent with license conditions can provide adequate or equivalent protection is immediately apparent.
> (2) during severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions can provide adequate or equivalent protection.

Suspended security measures should be reinstated as soon as conditions permit.

The suspension of security measures should be reported and documented in accordance with the provisions of § 73.71.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and

should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the onsite physical protection program, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Review and audit reports should be maintained and available for inspection, for a period of three (3) years.

Alternative measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 6 – Category II: Fixed Site Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The physical protection program should be designed to immediately detect attempts to remove SNM and provide sufficient delay through the use of barriers and/or armed responders to allow local law enforcement agencies to promptly recovery SNM.

The physical protection program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness.

Licensees should ensure that the design of the physical protection program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

In addition to these fixed-site requirements, the NRC may require, depending on the individual facility and site conditions, alternate or additional measures deemed necessary to protect against theft or diversion of Category II SNM. [1] [13]

Licensees should analyze and identify site-specific conditions that may affect the specific measures needed to implement the requirements of this section and should account for these conditions in the design of the physical protection program.

Upon the request of an authorized representative of the NRC, licensees should demonstrate the ability to meet NRC requirements through the implementation of the physical protection program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

Licensees should establish, maintain, and implement an access authorization program and should describe the program in the Physical Security Plan.

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions.

---

[13] Where applicable, a reference to existing regulations is provided at the end of the proposed measures. In addition, proposed measures developed with consideration of risk insights are noted with a “1”.

Security Plans

Licensees should develop, maintain and implement a Physical Security Plan that describes how they will meet the performance objective and physical protection requirements. [73.67(c)(1)]

Licensees should develop, maintain and follow a Training and Qualification Plan that describes how they will meet the criteria in Part 73, Appendix B, except for tactical response training and qualification.

Licensees should develop, maintain and implement a Safeguards Contingency Plan that describes how they will meet the criteria in Part 73, Appendix C.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans. .

Security Organization

Licensees should establish and maintain a security organization that is designed, staffed, trained, qualified and equipped to implement its physical protection program. [73.67(d)(8]

The security organization should follow a management system to oversee the physical protection program including having at least one member (onsite and available at all times) to direct activities.

Members of the security organization should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties.

Physical Barriers

Performance capabilities

Licensees should identify and analyze site-specific conditions to determine the specific use, type, function and placement of physical barriers needed to satisfy the general performance objective and requirements. The physical barriers should control access into facility areas, account for site specific conditions, perform their required functions, and provide deterrence, delay or support access control.

Category II SNM should be used, processed and stored within controlled access area that is located within a protected area.

Openings in any barrier should be secured and monitored to prevent exploitation of the opening consistent with the function of the barrier.

Bullet resistant barriers

The central alarm station should be bullet-resisting.

Isolation zone

An isolation zone should be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone should be designed and of sufficient size to permit observation and assessment of activities on either side of the protected area barrier. Obstructions that could prevent the licensee's capability to meet the observation and assessment requirements of this section should be located outside of the isolation zone.

The isolation zone should be monitored with intrusion detection equipment designed and capable of detecting both attempted and actual penetration of the protected area perimeter barrier before completed penetration of the protected area perimeter barrier.

The isolation zone should be monitored with assessment equipment designed to provide real-time and play- back/recorded video images of the detected activities before and after each alarm annunciation.

Protected area

The protected area perimeter should be protected by physical barriers that are designed and constructed to limit access into the protected area, channel personnel, vehicles and materials to designated access control portals, and be separate from any other physical barrier.

Penetrations through the protected area barrier should be secured and monitored to prevent and detect exploitation of the openings. All emergency exits in the protected area barrier should be alarmed and secured by locking devices. Where walls or roofs comprise a portion of the protected area perimeter barrier, an isolation zone is not necessary.

All exterior areas within the protected area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Controlled access area

The controlled access area perimeter should be protected by a physical barrier that is designed and constructed to limit access into the controlled access area, and channel personnel, vehicles and materials to designated access control portals.

Other than fuel elements or fuel assemblies, Category II SNM should be stored in tamper-indicating containers in a vault-type room, unless the material is being processed or personally attended. [73.67(d)(2)] Intermediate storage of Category II SNM during processing should be kept in locked compartments or locked process equipment, except when personally attended.

The vault-type room should be equipped with an intrusion detection capability.

Penetrations through the controlled access area barrier should be secured and monitored to prevent and detect exploitation of the openings.

All exterior areas within the controlled access area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Vehicle control measures

Licensees should design, construct, install and maintain a vehicle barrier system to include passive and active barriers, to prevent unauthorized access of vehicles into the protected area.

The operation of vehicle barriers should be periodically checked. A secondary power source or a means of mechanical or manual operation should be provided to ensure that active barriers can be placed in the denial position. Vehicle barriers should be periodically surveilled and observed to detect indications of tampering and degradation.

Where rail access is provided into the protected area, additional measures including installing a train derailer, removing a section of track, or restricting access to railroad sidings, should be provided.

Licensees should identify areas from which a waterborne vehicle should be restricted and install buoys, markers or other equipment to restrict access. Water approaches should be periodically surveilled and observed.

Access Controls

Performance capabilities

Licensees should control personnel, vehicle and material access at each access control point consistent with the function of each barrier as needed to satisfy the general performance objective and requirements. [73.67(d)(6)]

Access control portals should be located outside or concurrent with the physical barrier through which it controls access and should be equipped with locking devices, intrusion detection equipment, and surveillance equipment consistent with the intended function.
Licensees should provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment.

Licensees should establish, implement, and maintain a list of individuals who are authorized to have unescorted access to protected areas and controlled access areas. The list should include only those individuals who have a continued need for access to those areas in order to perform their duties and responsibilities. The list should be approved by a cognizant security manager, and updated and re-approved periodically.

Individuals responsible for performing the last access control function at each access control portals should be isolated to assure the ability to respond or summon assistance.

Licensees should limit unescorted access to the protected and controlled access areas to only individuals who require unescorted access to perform assigned duties and responsibilities.

Access control systems should be designed to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions. Licensees should implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

Protected areas

Licensees should, before granting access into protected areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements. [73.67(d)(4)] Licensees should exercise control over all vehicles inside the protected area to ensure that they are used only by authorized individuals and for authorized purposes. When not in use the vehicles keys should be removed or the vehicle should be otherwise disabled.

Vehicles transporting hazardous materials inside the protected area should be escorted by a member of the security organization.

Controlled access areas

Licensees should, before granting access into control access areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements. [73.67(d)(4)]

Licensees should exercise control over all vehicles inside the controlled access area to ensure that they are used only by authorized individuals and for authorized purposes.

Access control devices

Licensees should control all keys, locks, combination, passwords and related access control devices used to control access to protected areas and security systems to reduce the probability of compromise.

Access control devices should only be issued to individuals with unescorted access who require those devices to perform official duties and responsibilities. Licensees should maintain a list of individuals which have been issued access control devices and implement a process to account for access control devices at least annually. Upon less than favorable termination of employment, access control devices that were issued or accessed by that employee should be changed.

Licensees should implement compensatory measures upon discovery that any access control device may have been compromised. Compensatory measures should remain in effect until the potential compromise is corrected.

Licensees should implement a numbered photo identification badge program for all individuals authorized unescorted access to protected areas. Badges should be clearly displayed by all individuals inside protected areas. [73.67(d)(5)]

Licensees should maintain a record, to include name and areas to which unescorted access is granted, of all individuals issued photo identification.

Visitors

Licensees may permit escorted access to protected areas to individuals who have not been granted unescorted access. Licensees should develop and implement procedures for processing, escorting and controlling visitors which include confirmation of identity, listing of

visitors, issuance of a visitor badge, establishing escort ratios, monitoring visitor activities, and escorting visitors at all times. [73.67(d)(6 & 7)]

Licensees should ensure that all escorts are trained to perform escort duties, have unescorted access to areas in which they perform escort duties, and have a means of timely communication with security personnel to summon assistance if needed.

Individuals not employed by licensees who require frequent or extended unescorted access to protected areas to perform duties and responsibilities required by licensees should satisfy the access authorization requirements and be issued a non-employee photo identification badge.

Search Programs

Performance capabilities

Search programs should detect, deter and prevent the introduction of firearms, explosives, incendiary devices or other items which could be used to aid in the theft or diversion of SNM. Search programs should also detect, deter and prevent the removal or diversion of SNM.

Licensees should search all personnel, vehicles and materials requesting access to protected areas.

Search for firearms, explosives, incendiary devices or other contraband should be accomplished through the use of equipment capable of detecting those items, or through visual and physical search or both, to ensure that all items are clearly identified before granting access to protected areas. When search equipment is out of service, is not operating satisfactorily, or cannot be used effectively, a visual and physical search should be conducted.

When an attempt to introduce prohibited items has occurred or is suspected, licensees should implement actions to ensure that suspect individuals, vehicles and materials are denied access and should perform a visual and physical search to determine the absence or existence of a threat.

Licensees should develop and implement procedures for vehicle search at vehicle access portals to include searching the cab, engine compartment, under carriage and cargo areas.

Licensees should search personnel, vehicles and packages leaving the controlled access area and protected area for unauthorized or concealed SNM, and for metal or other shielding material. [73.67(d)(10)]

Federal, State and local law enforcement personnel on official duty are excepted from search requirements. Armed security officers who are on duty and have exited the protected area may re-enter the protected area without being searched for firearms.

Licensees may develop and implement exceptions to protected area search requirements for safety or operational reasons provided that the general performance objective and requirements are satisfied through specific security measures which could include positively controlling materials, storing SNM in locked areas, escorting SNM by an armed member of the security organization, verify material at off-loading.

Detection and Assessment Systems

Performance capabilities

Licensees should establish and maintain intrusion detection and assessment systems that satisfy the general performance objective and requirements and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the protective strategy. [73.67(d)(3)]

Intrusion detection and assessment systems should be designed to provide visual and audible annunciation of alarms, provide visual display to facilitate assessment, ensure alarm and annunciation of the type and location of the alarm, provide automatic indication when the alarm system or component fails or is operating on backup power, and support the initiation of a timely response.

Transmission lines should be tamper indicating and self-checking.

Intrusion detection and assessment equipment at the protected area perimeter and vault-type room(s) should remain operable from an uninterruptable power supply in the event of the loss of normal power.

Alarm Stations

Intrusion detection equipment should annunciate and video assessment equipment should display concurrently in at least one continuously staffed on-site alarm stations (i.e., central alarm station). A secondary alarm station, which may be located off-site, should be capable of periodically verifying the status of the central alarm station, verifying that the central alarm station has resolved alarms and summoning off-site assistance, if needed.

The central alarm station should be designed and equipped to ensure that a single act cannot disable the alarm station. The central alarm station wall, doors, ceiling, floor and windows should be bullet resisting. Licensees should ensure the survivability of the central alarm station to maintain the ability to perform its functions including detect and assess alarms, initiate and coordinate adequate response to alarms, summon off-site assistance, and provide command and control.

The central alarm station should be located in a protected area and should not be visible from the perimeter of the protected area.

Alarm stations should be continuously staffed with at least one trained and qualified alarm station operator who should not be assigned other duties or responsibilities which would interfere with the operator's ability to execute the functions of the alarm station.
Alarm station operators should assess and initiate response to all alarms and other events, as appropriate, in accordance with security plans and implementing procedures. Alarm station operators should maintain a record of all alarms.

Surveillance, observation and monitoring

The physical protection program should include surveillance, observation and monitoring as needed to satisfy the general performance objective and requirements, identify indications of tampering or otherwise implement the protective strategy.

Unattended openings that intersect a security boundary should be protected by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation.

Armed security patrols should periodically check external areas of the protected areas to include physical barriers.

Security personnel should be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Upon detection of tampering, licensees should initiate response in accordance with security plans and implementing procedures.

Illumination

Licensees should ensure that all areas of the facility are provided with illumination necessary to satisfy the general performance objective and requirements or otherwise implement the protective strategy.

Licensees should provide a minimum illumination level of 0.2 foot-candles, measured horizontally at ground level, in the isolation zone and appropriate exterior areas within the protected area. Alternatively, licensees may augment the facility illumination system by means of low-light technology.

Communication

Licensees should establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

Alarm station operators should be capable of calling for assistance in accordance with security plans and implementing procedures. [73.67(d)(9)]

All on-duty security force personnel should be capable of maintaining continuous communication with an individual in the central alarm station, and vehicle escorts should maintain continuous communication with security personnel. All personnel escorts should maintain timely communication with security personnel.

Alarm stations should be capable of two-way voice communication either directly or through an intermediary to local law enforcement using two independent means using different technologies.

Non-portable communications equipment should remain operable from independent power sources in the event of loss of normal power.

Licensees should identify site areas where communication could be interrupted or cannot be maintained and should establish alternative communication measures for those areas.

Response

Performance capabilities

Licensees should establish and maintain, at all times, properly trained, qualified and equipped personnel capable of interrupting unauthorized activities until local law enforcement arrives and to allow local law enforcement agencies to promptly recover SNM.

Licensees should ensure that all firearms, ammunition and equipment necessary to implement security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

Licensees should train each armed member of the security organization to interrupt unauthorized activities by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law.

Licensees should provide armed response personnel to carry out armed response duties within pre-determined time lines specified in the protective strategy.

Armed security officers

Armed security officers should be onsite and available at all times to carry out their assigned response duties.

The minimum number of armed security officers should be documented in security plans.
Protective Strategy

Licensees should establish, maintain and implement a written protective strategy in accordance with the requirements in Part 73, Appendix C. [73.67(d)(11)]

Upon receipt of an alarm or other indication of a threat, licensees should determine the existence and level of the threat in accordance with pre-established assessment methodologies, initiate response actions to immediately detect attempts to remove of SNM and provide sufficient delay through the use of barriers and/or armed responders to allow local law enforcement agencies to promptly recovery SNM in accordance with the requirements in Part 73, Appendix C, and notify law enforcement agencies in accordance with site procedures.

Law enforcement liaison

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. To the extent practicable, licensees should conduct annual local law enforcement site familiarization activities to include a review of the protective strategy and on-site and off-site response procedures, and joint response exercises.

Heightened security

Licensees should establish, maintain and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

Licensees should ensure that the specific protective measures and actions identified for each threat level are consistent with security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat.

Security Program Review

Licensees should conduct an exercise at least every 12 months to test the performance and effective implementation of its protective strategy and physical security procedures.

Licensees should review each element of the physical security program at least every 24 months based upon site-specific analysis, assessments or other performance indicators. The reviews should be conducted by individuals independent of the physical security program.

Reviews should be conducted within 12 months following initial implementation or a change in personnel, procedures, equipment or facilities that potentially could adversely affect security.

Reviews should include an audit of the effectiveness of the physical security program, security plans, implementing procedures, safety/safeguards interface activities, the testing and maintenance program, and response commitments by local, State and Federal law enforcement authorities.

The results and recommendations of these reviews, management findings regarding the program and any actions taken as a result of previous program reviews should be documented in a report to facility and corporate management. These reports should be maintained in an auditable form and available for inspection.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptable power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions. [73.46(g), 73.46(g)(4), 73.46(g)(5)]

The maintenance and testing program should be described in security plans.

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented.

Licensees should test each intrusion alarm for operability at the beginning and end of any period that it is used or, for continuous operation, at least once every seven days.

Intrusion detection and access control equipment should be performance tested in accordance with security plans and implementing procedures.

Onsite communication equipment should be tested for operability not less frequently than once at the beginning of each security personnel work shift. Communication systems between alarm stations and local law enforcement agencies, including backup communication, should be tested for operability at least once per day.

Search equipment should be tested for operability at least once each day and tested for performance at least during each seven day period.

Security equipment or systems should be testing in accordance with the site maintenance, testing and calibration procedures before being place in service (pre-operational), or before being placed back in service after each repair or inoperable state.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the physical security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in security plans and should not be used in lieu of performing timely maintenance.

Suspension of security measures

Licensees may suspend implementation of affected requirements under the following conditions:

> (1) when suspension of security measures is immediately needed to protect the public health and safety and no action consistent with license conditions can provide adequate or equivalent protection is immediately apparent.
> (2) during severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions can provide adequate or equivalent protection.

Suspended security measures should be reinstated as soon as conditions permit.

The suspension of security measures should be reported and documented in accordance with the provisions of § 73.71.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the onsite physical protection program, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Review and audit reports should be maintained and available for inspection, for a period of three (3) years.

Alternative measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 7 – Category II – Moderately dilute: Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The physical protection program should be designed to promptly detect attempts to remove of SNM and notify allow local law enforcement agencies to allow the recovery of SNM.

The physical protection program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness.

Licensees should ensure that the design of the physical protection program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

In addition to these fixed-site requirements, the NRC may require, depending on the individual facility and site conditions, alternate or additional measures deemed necessary to protect against theft or diversion of Category II - moderately dilute SNM.

Licensees should analyze and identify site-specific conditions that may affect the specific measures needed to implement the requirements of this section and should account for these conditions in the design of the physical protection program.

Upon the request of an authorized representative of the NRC, licensees should demonstrate the ability to meet NRC requirements through the implementation of the physical protection program, including the ability of security personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

Licensees should establish, maintain, and implement an access authorization program and should describe the program in the Physical Security Plan.

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions.

Security Plans

Licensees should develop, maintain and implement a Physical Security Plan that describes how they will meet the performance objective and physical protection requirements.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans.

Security Organization

Licensees should establish and maintain a security organization that is designed, staffed, trained, qualified and equipped to implement its physical protection program.

The security organization should follow a management system to oversee the physical protection program.

Members of the security organization should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties.

Physical Barriers

Performance capabilities

Licensees should identify and analyze site-specific conditions to determine the specific use, type, function and placement of physical barriers needed to satisfy the general performance objective and requirements. The physical barriers should control access into facility areas, account for site specific conditions, perform their required functions, and provide deterrence, delay or support access control.

Category II - moderately dilute SNM should be used, processed and stored within a controlled access area.

Openings in any barrier should be secured and monitored to prevent exploitation of the opening consistent with the function of the barrier.

Controlled access area
The controlled access area perimeter should be protected by a physical barrier that is designed and constructed to limit access into the controlled access area, and channel personnel, vehicles and materials to designated access control portals.

Other than fuel elements or fuel assemblies, Category II - moderately dilute SNM should be stored in tamper-indicating containers in a vault-type room, unless the material is being processed or personally attended. Intermediate storage of Category II - moderately dilute SNM during processing should be kept in locked compartments or locked process equipment, except when personally attended.

Vault-type rooms should use intrusion detection systems.

Penetrations through the controlled access area barrier should be secured and monitored to prevent and detect exploitation of the openings consistent with the function of the barrier.

All exterior areas within the controlled access area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Access Controls

Performance capabilities

Licensees should control personnel, vehicle and material access at each access control point consistent with the function of each barrier as needed to satisfy the general performance objective and requirements.

Access control portals should be located outside or concurrent with the physical barrier through which it controls access and should be equipped with locking devices, and surveillance equipment consistent with the intended function.

Licensees should provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment.

Licensees should limit unescorted access to controlled access areas to only individuals who require unescorted access to perform assigned duties and responsibilities.

Access control systems should be designed to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions. Licensees should implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

Controlled access areas

Licensees should, before granting access into control access areas, confirm the identity of individuals; verify the authorization for access of individuals, vehicles, and materials; and search individuals, vehicles and material consistent with the search requirements.

Licensees should exercise control over all vehicles inside the controlled access area to ensure that they are used only by authorized individuals and for authorized purposes.

Access control devices

Licensees should control all keys, locks, combination, passwords and related access control devices used to control access to controlled access areas and security systems to reduce the probability of compromise.

Access control devices should only be issued to individuals with unescorted access who require those devices to perform official duties and responsibilities. Licensees should maintain a list of individuals which have been issued access control devices and implement a process to account for access control devices at least annually. Upon less than favorable termination of employment, access control devices that were issued or accessed by that employee should be changed.

Licensees should implement compensatory measures upon discovery that any access control device may have been compromised. Compensatory measures should remain in effect until the potential compromise is corrected.

Licensees should implement a numbered photo identification badge program for all individuals authorized unescorted access to controlled access areas. Badges should be clearly displayed by all individuals inside controlled access areas.

Licensees should maintain a record, to include name and areas to which unescorted access is granted, of all individuals issued photo identification.

Visitors

Licensees may permit escorted access to controlled access areas to individuals who have not been granted unescorted access. Licensees should develop and implement procedures for processing, escorting and controlling visitors which include confirmation of identity, listing of visitors, issuance of a visitor badge, establishing escort ratios, monitoring visitor activities, and escorting visitors at all times.

Licensees should ensure that all escorts are trained to perform escort duties, have unescorted access to areas in which they perform escort duties, and have a means of timely communication with security personnel to summon assistance if needed.

Individuals not employed by licensees who require frequent or extended unescorted access to controlled access areas to perform duties and responsibilities required by licensees should satisfy the access authorization requirements and be issued a non-employee photo identification badge.

Search Programs

Performance capabilities

Search programs should detect, deter and prevent the introduction of firearms, explosives, incendiary devices or other items which could be used to aid in the theft or diversion of SNM. Search programs should also detect, deter and prevent the removal or diversion of SNM.

Controlled access area

Licensees should randomly search personnel, vehicles and materials requesting access to controlled access areas. The frequency and methods of entry searches should consider the forms and means of access to the SNM.

Search for firearms, explosives, incendiary devices or other contraband should be accomplished through the use of equipment capable of detecting those items, or through visual and physical search or both, to ensure that all items are clearly identified before granting access to controlled access areas. When search equipment is out of service, is not operating satisfactorily, or cannot be used effectively, a visual and physical search should be conducted.

When an attempt to introduce prohibited items has occurred or is suspected, licensees should implement actions to ensure that suspect individuals, vehicles and materials are denied access and should perform a visual and physical search to determine the absence or existence of a threat.

Licensees should search personnel, vehicles and packages leaving the controlled access area for unauthorized or concealed SNM, and for metal or other shielding material. The frequency and methods of exit searches should consider the forms and means of access to the SNM.

Federal, State and local law enforcement personnel on official duty are excepted from search requirements.

Licensees may develop and implement exceptions to controlled access area search requirements for safety or operational reasons provided that the general performance objective and requirements are satisfied through specific security measures which could include positively controlling materials, storing in locked areas, escorting by a member of the security organization, verify material at off-loading.

Detection and Assessment Systems

Performance capabilities

Licensees should establish and maintain intrusion detection and assessment systems that satisfy the general performance objective and requirements and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the protective strategy.

The controlled access area barrier should either:

(1) be monitored with an intrusion detection equipment.

or

(2) by periodic patrols to detect unauthorized penetrations or activities.
Security patrols should periodically check external areas of the controlled access areas to include physical barriers and access portals.

Intrusion detection and assessment systems should be designed to provide visual and audible annunciation of alarms, provide visual display to facilitate assessment, ensure alarm and annunciation of the type and location of the alarm, provide automatic indication when the alarm system or component fails or is operating on backup power, ensure that an alarm station operator cannot change the status of a detection point or deactivate a locking or access control device without the knowledge and concurrence of the other alarm station operator and support the initiation of a timely response.

Transmission lines should be tamper indicating and self-checking.

Intrusion detection and assessment equipment at vault type rooms should remain operable from an uninterruptable power supply in the event of the loss of normal power.

Alarm Stations

Intrusion detection equipment should annunciate and video assessment equipment should display concurrently in a continuously staffed on-site alarm station (i.e., central alarm station).

The central alarm station should be designed and equipped to ensure that a single act cannot disable the alarm station. The central alarm station wall, doors, ceiling, floor and windows should be bullet resisting. Licensees should ensure the survivability of the central alarm station to maintain the ability to perform its functions including detect and assess alarms, initiate and coordinate adequate response to alarms, summon off-site assistance, and provide command and control.

The central alarm station should be located in a controlled access area and should not be visible from the perimeter of the controlled access area.

The central alarm station should be continuously staffed with at least one trained and qualified alarm station operator who should not be assigned other duties or responsibilities which would interfere with the operator's ability to execute the functions of the alarm station.

Alarm station operators should assess and initiate response to all alarms and other events, as appropriate, in accordance with security plans and implementing procedures. Alarm station operators should maintain a record of all alarms.

Surveillance, observation and monitoring

The physical protection program should include surveillance, observation and monitoring as needed to satisfy the general performance objective and requirements, identify indications of tampering or otherwise implement the protective strategy.

Unattended openings that intersect a security boundary should be protected by intrusion detection equipment or observed by security personnel at a frequency sufficient to detect exploitation.

Security patrols should periodically check external areas of the controlled access areas to include physical barriers.

Security personnel should be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Upon detection of tampering, licensees should initiate response in accordance with security plans and implementing procedures.

Communication

Licensees should establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

Alarm station operators should be capable of calling for assistance in accordance with security plans and implementing procedures.

All on-duty security force personnel should be capable of maintaining continuous communication with an individual in the central alarm station, and vehicle escorts should maintain continuous communication with security personnel. All personnel escorts should maintain timely communication with security personnel.

Alarm stations should be capable of two-way voice communication either directly or through an intermediary to local law enforcement using two independent means using different technologies.

Non-portable communications equipment should remain operable from independent power sources in the event of loss of normal power.

Licensees should identify site areas where communication could be interrupted or cannot be maintained and should establish alternative communication measures for those areas.

Response

Performance capabilities

Licensees should establish and maintain properly trained, qualified and equipped personnel capable of promptly detecting attempts to remove of SNM and notify allow local law enforcement agencies to allow the recovery of SNM.

Protective Strategy

Licensees should ensure that a member of the security organization or offsite response force responds to all unauthorized penetrations or activities in accordance with security plans and response procedures.

Upon receipt of an alarm or other indication of a threat, licensees should determine the existence and level of the threat in accordance with pre-established assessment methodologies, initiate response actions to promptly detect attempts to remove of SNM and notify local law enforcement agencies to recovery SNM in accordance site procedures.

Law enforcement liaison

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. To the extent practicable, licensees should conduct annual local law enforcement site familiarization activities to include a review of the protective strategy and on-site and off-site response procedures, and joint response exercises.

Heightened security

Licensees should establish, maintain and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat.

Licensees should ensure that the specific protective measures and actions identified for each threat level are consistent with security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat.

Security Program Review

Licensees should conduct an exercise at least every 12 months to test the performance and effective implementation of its protective strategy and physical security procedures.

Licensees should review each element of the physical security program at least every 24 months based upon site-specific analysis, assessments or other performance indicators. The reviews should be conducted by individuals independent of the physical security program.

Reviews should be conducted within 12 months following initial implementation or a change in personnel, procedures, equipment or facilities that potentially could adversely affect security.

Reviews should include an audit of the effectiveness of the physical security program, security plans, implementing procedures, safety/safeguards interface activities, the testing and maintenance program, and response commitments by local, State and Federal law enforcement authorities.

The results and recommendations of these reviews, management findings regarding the program and any actions taken as a result of previous program reviews should be documented in a report to facility and corporate management. These reports should be maintained in an auditable form and available for inspection.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment, including secondary and uninterruptable power supplies, are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

The maintenance and testing program should be described in security plans

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented.

Licensees should periodically test each intrusion alarm for operability.

Intrusion detection and access control equipment should be performance tested in accordance with security plans and implementing procedures.

Onsite communication equipment should be tested for operability not less frequently than once at the beginning of each security personnel work shift. Communication systems between alarm stations and local law enforcement agencies, including backup communication, should be tested for operability at least once per day.

Search equipment should be periodically tested for operability and for performance.

Security equipment or systems should be testing in accordance with the site maintenance, testing and calibration procedures before being place in service (pre-operational), or before being placed back in service after each repair or inoperable state.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the physical security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in security plans and should not be used in lieu of performing timely maintenance.

Suspension of security measures

Licensees may suspend implementation of affected requirements under the following conditions:

> (1) when suspension of security measures is immediately needed to protect the public health and safety and no action consistent with license conditions can provide adequate or equivalent protection is immediately apparent.
> (2) during severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions can provide adequate or equivalent protection.

Suspended security measures should be reinstated as soon as conditions permit.

The suspension of security measures should be reported and documented in accordance with the provisions of § 73.71.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the onsite physical protection program, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Review and audit reports should be maintained and available for inspection, for a period of three (3) years.

Alternative measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 8 – Category III: Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The physical protection program should be designed to timely detect attempts to remove of SNM and notify local law enforcement agencies to allow recovery of the SNM.

Licensees should analyze and identify site-specific conditions that may affect the specific measures needed to implement the requirements of this section and should account for these conditions in the design of the physical protection program.

Licensee should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program.

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during normal conditions and minimize conflict during emergency conditions. [1][14]

Security Plans

Licensees should develop, maintain and implement a Physical Security Plan and implementing procedures that describes how they will meet the performance objective and physical protection requirements. [73.67(c)(1), 73.67(f)(4)]

NRC approval of the Physical Security Plan is required for the following types and quantities:

- For Category III SNM, equal or greater than 250 g plutonium or uranium-233; and
- For Category III SNM, equal or greater than 350 g uranium-235 contained in high enriched uranium; equal or greater than 1 kg uranium-235 in uranium enriched to equal or greater than 10 percent U-235 but less than 20 percent; or equal or greater than 10 kg uranium-235 in uranium enriched to greater than natural but below 10 percent U-235.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans.

[14] Where applicable, a reference to existing regulations is provided at the end of the proposed measures. In addition, proposed measures developed with consideration of risk insights are noted with a “1” and proposed measures developed with consideration of security orders are noted with a “2”.

Security Organization

Licensees should establish and maintain a security organization that is designed, staffed, trained, qualified and equipped to implement its physical protection program.

The security organization should follow a management system to oversee the physical protection program.

Members of the security organization should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties.

Physical Barriers

Performance capabilities

Licensees should identify and analyze site-specific conditions to determine the specific use, type, function and placement of physical barriers needed to satisfy the general performance objective and requirements. The physical barriers should control access into facility areas, account for site specific conditions, perform their required functions, and provide deterrence, delay or support access control.

Controlled access area

The controlled access area perimeter should include a physical barrier that is designed and constructed to limit access into the controlled access area, and channel personnel, vehicles and materials to designated access control portals.

Penetrations through the controlled access area barrier should be secured and monitored to prevent and detect exploitation of the openings consistent with the function of the barrier.

All exterior areas within the controlled access area should be periodically checked to detect and deter unauthorized personnel, vehicles and materials.

Category III SNM should be used, processed and stored within a controlled access area. [73.67(f)(1)]

Access Controls

Performance capabilities

Licensees should control personnel, vehicle and material access at each access control point consistent with the function of each barrier as needed to satisfy the general performance objective and requirements.

Access control portals should be located outside or concurrent with the physical barrier through which it controls access and should be equipped with locking devices, and surveillance equipment consistent with the intended function.

Licensees should provide supervision and control over the badging process to prevent unauthorized bypass of access control equipment.

Licensees should limit unescorted access to the controlled access area to only individuals who require unescorted access to perform assigned duties and responsibilities.
Access control systems should be designed to accommodate the potential need for rapid ingress or egress of authorized individuals during emergency conditions or situations that could lead to emergency conditions. Licensees should implement security procedures to ensure that authorized emergency personnel are provided prompt access to affected areas and equipment.

Controlled access areas

Licensees should, before granting access into controlled access areas, confirm the identity of individuals; and verify the authorization for access of individuals, vehicles, and materials.

Access control devices

Licensees should control all keys, locks, combination, passwords and related access control devices used to control access to controlled access areas and security systems to reduce the probability of compromise.

Access control devices should only be issued to individuals with unescorted access who require those devices to perform official duties and responsibilities. Licensees should maintain a list of individuals which have been issued access control devices and implement a process to account for access control devices at least annually. Upon less than favorable termination of employment, access control devices that were issued or accessed by that employee should be changed.

Licensees should implement compensatory measures upon discovery that any access control device may have been compromised. Compensatory measures should remain in effect until the compromise is corrected.

Licensees should implement a numbered photo identification badge program for all individuals authorized unescorted access to controlled access areas. Badges should be clearly displayed by all individuals inside controlled access areas.

Licensees should maintain a record, to include name and areas to which unescorted access is granted, of all individuals issued photo identification. [2]

Visitors

Licensees may permit escorted access to controlled access areas to individuals who have not been granted unescorted access. Licensees should develop and implement procedures for processing, escorting and controlling visitors which include confirmation of identity, listing of visitors, issuance of a visitor badge, establishing escort ratios, monitoring visitor activities, and escorting visitors at all times.

Licensees should ensure that all escorts are trained to perform escort duties, have unescorted access to areas in which they perform escort duties, and have a means of timely communication with security personnel to summon assistance if needed.

Individuals not employed by licensees who require frequent or extended unescorted access to controlled access areas to perform duties and responsibilities required by licensees should satisfy the access authorization procedures and be issued a non-employee photo identification badge.

Detection and Assessment Systems

Performance capabilities

Licensees should establish and maintain intrusion detection and assessment systems that satisfy the general performance objective and requirements and provide the capability to detect and assess unauthorized persons and facilitate the protective strategy. [73.67(f)(2)]

The controlled access area barrier should either:

(1) be monitored with an intrusion detection equipment. [73.67(f)(2)]

Intrusion detection systems should be designed to provide visual and audible annunciation of alarms, ensure alarm and annunciation of the type and location of the alarm, provide automatic indication when the alarm system or component fails or is operating on backup power and support the initiation of a timely response. Assessment of intrusion detection alarms should be performed by a member of the security organization.

or

(2) by periodic patrols to detect unauthorized penetrations or activities. [73.67(f)(2)]

Security patrols should periodically check external areas of the controlled access areas to include physical barriers and access portals.

The physical protection program should include surveillance, observation and monitoring as needed to satisfy the general performance objective and requirements, or identify indications of tampering.

Security personnel should be trained to recognize obvious indications of tampering consistent with their assigned duties and responsibilities. Upon detection of tampering, licensees should initiate response in accordance with security plans and implementing procedures.

Communication

Licensees should establish and maintain continuous communication capability with onsite and offsite resources to ensure effective command and control during both normal and emergency situations.

A designated member of the security organization should be capable of calling for assistance in accordance with security plans and implementing procedures. Communication should be by two-way voice communication either directly or through an intermediary to local law enforcement using two independent means using different technologies.

All on-duty security force personnel should be capable of maintaining continuous communication with the individual responsible for requesting assistance. All personnel escorts should maintain timely communication with security personnel.

Non-portable communications equipment should remain operable from independent power sources in the event of loss of normal power.
Licensees should identify site areas where communication could be interrupted or cannot be maintained and should establish alternative communication measures for those areas.

Response

Licensees should ensure that a member of the security organization or offsite response force responds to all unauthorized penetrations or activities in accordance with security plans and response procedures. [73.67(f)(3)]

Law enforcement liaison

To the extent practicable, licensees should document and maintain current agreements with applicable law enforcement agencies to include estimated response times and capabilities. [2]
To the extent practicable, licensees should conduct annual local law enforcement site familiarization activities to include a review of the protective strategy and on-site and off-site response procedures, and joint response exercises.

Heightened security

Licensees should establish, maintain and implement a threat warning system which identifies specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat. [2]

Licensees should ensure that the specific protective measures and actions identified for each threat level are consistent with security plan and other emergency plans and procedures. Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat. [2]

Security Program Review

Licensees should review each element of the physical security program at least every 24 months based upon site-specific analysis, assessments or other performance indicators. The reviews should be conducted by individuals independent of the physical security program.

Reviews should be conducted within 12 months following initial implementation or a change in personnel, procedures, equipment or facilities that potentially could adversely affect security.

Reviews should include an audit of the effectiveness of the physical security program, security plans, implementing procedures, safety/safeguards interface activities, and response commitments by local, State and Federal law enforcement authorities.

The results and recommendations of these reviews, management findings regarding the program and any actions taken as a result of previous program reviews should be documented in a report to facility and corporate management. These reports should be maintained in an auditable form and available for inspection.

Maintenance and Testing

Performance capabilities

For any security systems and equipment, licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

The maintenance and testing program should be described in security plans.

Onsite communication equipment should be periodically tested for operability. Communication systems between the facility and local law enforcement agencies, including backup communication, should be tested for operability periodically. [2]

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the physical security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in security plans and should not be used in lieu of performing timely maintenance.

Suspension of security measures

Licensees may suspend implementation of affected requirements under the following conditions:

> (1) when suspension of security measures is immediately needed to protect the public health and safety and no action consistent with license conditions can provide adequate or equivalent protection is immediately apparent.
> (2) during severe weather when the suspension of affected security measures is immediately needed to protect the personal health and safety of security force personnel and no other immediately apparent action consistent with the license conditions can provide adequate or equivalent protection.

Suspended security measures should be reinstated as soon as conditions permit.

The suspension of security measures should be reported and documented in accordance with the provisions of § 73.71.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the onsite physical protection program, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Review and audit reports should be maintained and available for inspection, for a period of three (3) years.

Alternative measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 9 – Additional Physical Protection Mesusures for 1) Category III Quantities of Plutonium-239, 2) Small Quantities of Spent Nuclear Fuel and 3) non-power reactor facility sabotage

In addition to the Category III physical protection requirements for theft or diversion, licensees that possess aggregated Category III quantities of plutonium-239 greater than 250 grams and of spent nuclear fuel less than 100 grams should implement the following requirements. Note all plutonium-238, both sealed and unsealed would be subject to the requirements in Part 37. Other plutonium isotopes would not be subject to these additional requirements.

Access Authorization

A licensee's access authorization program should include the requirements in §73.57, §73.59, and §73.61; and access authorization requirements essentially the same as requirements in §37.23, §37.25, §37.31, and §37.33.

Detection and Assessment

Licensees should establish and maintain the capability to continuously monitor and detect without delay all unauthorized entries into areas containing aggregated plutonium-239 greater than 250 grams or aggregated spent nuclear fuel less than 100 grams. (Note, this may be the entire controlled access area or another controlled access area specifically for these materials.)

Licensees should provide the means to maintain continuous monitoring and detection capability in the event of a loss of the primary power source, or provide for an alarm and response in the event of a loss of this capability to continuously monitor and detect unauthorized entries.

Monitoring and detection may be performed by:

1. A monitored intrusion detection system that includes electronic devices such as sensors or detectors (e.g. radiation alarms) that is linked to an onsite or offsite central monitoring facility; or
2. Electronic devices such as sensors or detectors for intrusion detection alarms that will alert nearby facility personnel; or
3. A monitored video surveillance system; or
4. Direct visual surveillance by approved individuals located within the security zone; or
5. Direct visual surveillance by a licensee designated individual located outside the security zone.

Licensee should have a means to detect unauthorized removal of plutonium by:

1. Electronic sensors linked to an alarm; or
2. Continuous monitored video surveillance; or
3. Direct visual surveillance.

Licensees should immediately assess each actual or attempted unauthorized entry into the security zone to determine whether the unauthorized access was an actual or attempted theft, sabotage, or diversion.

Non-power reactors sabotage

Non-power reactors licensees with power levels greater than 2 megawatts should implement the following requirements.

Licensees should analyze the impact and stand-off distances from vehicle borne attacks and construct, install and maintain a vehicle barrier system to include passive and active barriers adequate to protect personnel, equipment, and systems, if necessary. [2]

The operation of vehicle barriers should be periodically checked. A secondary power source or a means of mechanical or manual operation should be provided to ensure that active barriers can be placed in the denial position. Vehicle barriers should be periodically surveilled and observed to detect indications of tampering and degradation.

Where rail access is provided into the controlled access area, additional measures including installing a train derailer, removing a section of track, or restricting access to railroad sidings, should be provided.

Licensees should ensure alternate coolant sources to mitigate damage to non-power reactor fuel and radiological release to the public.

Attachment 10 – Category I: Transportation Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a transportation security program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. [73.26(a)]

The transportation security program should protect against the design basis threats of theft and diversion and radiological sabotage as stated in §73.1 and should be designed to prevent the removal of Category I SNM and other unauthorized activities involving SNM. [73.1]

The transportation security program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness. The program should address the security of the material from the custody transfer time at the point of departure and until the custody transfer time at destination.

In addition to these transportation security requirements, the NRC may require, depending on the individual transport conditions, alternate or additional measures deemed necessary to protect against theft and diversion or sabotage of Category I SNM. [73.26(a)]

Licensees should ensure that the design of the transportation security program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the transportation security program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures. [73.26(d)(4)]

Licensees should establish, maintain, and implement a performance evaluation program in accordance with Part 73, Appendix B to demonstrate and assess the effectiveness of the armed personnel in implementing the protective strategy.

Licensees should establish, maintain, and implement an access authorization program in accordance with 10 CFR Part 11 and should describe the program in the Transportation security Plan.

Licensee should establish, maintain, and implement an insider mitigation program and should describe the program in the Transportation security Plan. The insider mitigation program should monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to transportation security systems, movement control centers, and SNM transfer areas, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent theft and diversion or radiological sabotage.

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

Transportation Security Plan

Licensees should develop, maintain and implement an NRC-approved transportation security plan that describes how they will meet the performance objective and transportation security requirements. [73.20(c)]

Licensees should develop, maintain and follow a Training and Qualification Plan that describes how they will meet the criteria in Part 73, Appendix B. [73.26(d)(4)]

Licensees should develop, maintain and implement a Safeguards Contingency Plan that describes how they will meet the criteria in Part 73, Appendix C. [73.26(e)]

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the transportation security requirements and security plans. [73.26(d)(3)]

Security Organization

Licensees or their agents should establish and maintain a transportation security organization that is designed, staffed, trained, qualified and equipped to implement its transportation security program. [73.26(d)(1)]

Members of the security organization including armed escorts, armed response personnel or guards, and movement control center staff, should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties. [73.26(d)(1), 73.26(d)(4)]

The transportation security organization should follow a management system to oversee the transportation security program including having at least one member at the movement control center during the course of any shipment to direct transportation-security related activities. [73.26(d)(2), 73.26(d)(3)]

Notifications

Licensees or their agents should provide advance notification to the receiver of any planned shipment specifying the mode of transport, estimated time of arrival, and location of the nuclear material transfer point.

Licensees or their agents should receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport.

Licensees or their agents should provide advance notification to NRC in accordance with §73.72

Licensees or their agents should notify NRC and the receiver of the commencement of the shipment.

Transportation Route

The transportation security plan should include a description of the transportation route, including the location of SNM tranfer points, safe havens, and response forces. [73.26(i)]

Shipments should be scheduled to avoid regular patterns and preplanned to avoid areas of natural disaster, civil disorders, or other security threats. Shipments should be planned in order to minimize the number of material transfers and the storage time, and to assure that deliveries occur at a time when the receiver is present to accept the shipment. [73.26(b)(1)]

Arrangements should be made with law enforcement authorities or other response forces along the route of shipments for their response to an emergency or a call for assistance. [73.26(b)(2)]

Security arrangements for each shipment should be approved by the NRC prior to submitting the seven-day notice required by §73.72. Information to be supplied to the Commission in addition to the general security plan information is as follows:

> Shipper, consignee, carriers, transfer points, modes of shipment, point where escorts will relinquish responsibility or will accept responsibility for the shipment, arrangements made for transfer of shipment security, and security arrangements at point where escorts accept responsibility for an import shipment. [73.26(b)(3)]

Transportation Security System

Shipments of Category I SNM should be conducted utilizing transportation security systems including a closed and locked conveyance featuring a specially designed transportation security compartment, SNM containers, secure tiedowns, and physical protection features.

- The transportation security system should provide for immediate detection of attempts to compromise the integrity of the transportation compartment and access SNM containers.
- The transportation security system should provide resistance to and delay of access to Category I SNM necessary to achieve the performance objectives of §73.1(a).
- The transportation security system should provide for continuous determination of the position of the shipment and communication of the positioning information to the movement control center.

Category I SNM should be shipped in containers that are protected by tamper-indicating seals. The containers should also be locked if they are not in another locked container, compartment or transport. The outermost container or transport should be protected by tamper-indicating seals. [73.26(g)(3)]

The integrity of locks and seals should be checked before departure, during intermodal transfers, and upon arrival.

For shipment by road, design features of the truck or trailer should permit immobilization of the truck or of the cargo-carrying portion of the vehicle. The cab of the cargo vehicle should be armored. [73.26(i)(3)]

For shipment by air, shipments of Category I SNM should be conducted on an exclusive-use cargo aircraft in a secure and locked compartment or container.

For shipment by rail, shipments should be made in a freight train in an exclusive use fully closed and locked conveyance.

For shipment by sea, shipments should be made only on an exclusive-use transport vessel.

Access Controls

Performance capabilities

Licensees should control access to SNM loading and transfer areas, transportation security systems, transport and escort vehicles, aircraft, rail cars, and containers where Category I material is located as needed to satisfy the general performance objective and requirements. [73.26(g)(2)]

Licensees should implement a numbered photo identification badge program for all individuals who will have custody of a shipment. Badges should be clearly displayed by all individuals. [73.26(g)(1)]

Prior to transfer, the shipment should only be released when the individual who is in possession of the shipment has assured positive identification of all of the persons assuming custody of the shipment. [73.26(g)(1)]

Licensees should develop and implement procedures for search of conveyance and escort vehicles prior to loading. The conveyance and escort vehicles should be searched for explosives, incendiary devices and other items and conditions that have the potential of compromising the shipment. [73.26(i)(5)] Following the search, the conveyance must remain inside a controlled access area or under continuous surveillance.

Licensees should limit unescorted access to the protected and controlled access areas, transports, escort vehicles, aircraft, rail cars, to only individuals who require unescorted access to perform assigned duties and responsibilities.

Licensees should control all keys, locks, combination, passwords and related access control devices to reduce the probability of compromise.

Movement Control Center

The transportation security program should include a movement control center staffed and equipped to monitor and control Category I SNM shipments, to communicate with law enforcement authorities, and to respond to safeguards contingencies.

The movement control center should be staffed continuously by at least two individuals who will actively monitor the progress of the shipment with one individual having the authority to coordinate the physical protection activities.

The movement control center personnel must monitor the shipment continuously, i.e., 24-hours per day, from the time the shipment commences, or if delivered to a carrier for transport, from the time of delivery of the shipment to the carrier, until safe delivery of the shipment at its final destination, and must immediately notify the appropriate agencies in the event of a safeguards event under the provisions of § 73.71 of this part. Monitoring should include the use of shipment positioning information and voice communication to maintain information about the shipment's position and status.

The movement control center personnel and the armed escorts must maintain a written log for each shipment, which will include information describing the shipment and significant events that occur during the shipment. The log must be available for review by authorized NRC personnel for a period of at least 3 years following completion of the shipment.

Licensees should limit unescorted access to the movement control center to only individuals who require unescorted access to perform assigned duties and responsibilities. No single adversary action should prevent the movement control center from performing its functions.

Communication

The Category I SNM conveyance and each escort vehicle should be equipped with redundant communication capabilities that provide 2-way secure communications between the conveyance, the escort vehicle(s), the movement control center, and one another. To ensure that 2-way communication is possible at all times, alternate communications should not be subject to the same failure modes as the primary communication. [73.26(f)(2)]

Shipment personnel and the movement control center should be equipped with communication abilities that provide communications with law enforcement agencies and response forces along the route. [73.26(e)(2)]

Response

Performance capabilities

Licensees should establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats up to and including the design basis threats for theft and diversion and radiological sabotage to prevent the theft of Category I SNM

and other unauthorized activities involving SNM [and to provide for recovery of stolen SNM]. [73.26(e)(3)]

Licensees should ensure that all firearms, ammunition and equipment necessary to implement security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

Licensees should train each armed member of the transportation security organization to prevent or impede acts of theft and diversion and radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law. [73.26(e)(2)]

Licensees should provide tactical armed response personnel consisting of armed escorts which may be augmented by additional personnel to carry out armed response duties and execute the protective strategy.

The minimum number of armed response personnel should be documented in the transportation security plan. Armed response personnel should have knowledge of features and operations of the transport sufficient for execution of the protective strategy.

Tactical Responders

Licensees should determine the minimum number of tactical response personnel to satisfy the general performance objectives and requirements and implement the protective strategy.

Tactical response team members should be available for immediate response at all times during the transportation of the material and may not be assigned other duties or responsibilities that could interfere with their assigned response duties. Licensees should designate an individual who is responsible for directing the tactical response.

<u>Export/import shipments</u>

Licensees who import Category I SNM should make arrangements to assure that the material will be protected in transit as follows:

- An individual designated by the licensee or his agent, or as specified by a contract of carriage, should confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier. [73.26(c)(4)]
- The shipment should be protected at all times within the geographical limits of the United States as provided in this section and § 73.27. The licensee should retain each required record for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to ship this material, and superseded material for three years after each change. [73.26(c)(1)]

Licensees who export Category I SNM should comply with the transportation security requirements, as applicable, up to the first point where the shipment is taken off the transport outside the United States. The licensee should retain each record required by these sections for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to export this material, and superseded material for three years after each change. [73.26(c)(2)]

Heightened Security

Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.

Security Program Review

The transportation security program should be reviewed at least every 12 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program. [73.26(h)(6)]

The review should include an audit of transportation security procedures and practices, an evaluation of the effectiveness of the transportation security system, an audit of the transportation security system testing and maintenance program, and an audit of commitments established for response by local law enforcement authorities. [73.26(h)(6)]

The results and recommendations of the review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, should be documented in a report to the responsible organization management and to corporate management at least one level higher than that having responsibility for the day-to-day operation. [73.26(h)(6)]

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions. [73.26(h)(6)]

The maintenance and testing program should be described in transportation security plans.

During installation and construction of physical protection related components, licensees should assure that they comply with their respective design criteria and performance specifications. [73.26(h)(1)]

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented . [73.26(h)(4) and (5)]

Preoperational tests and inspections should be conducted for physical protection related subsystems and components to demonstrate their effectiveness, availability, and reliability with respect to their respective design criteria and performance specifications. [73.26(h)(2)]

Operational tests and inspections should be conducted for physical protection related subsystems and components to ensure that they are maintained in an operable and effective condition. [73.26(h)(3)]

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the transportation security program. [73.26(f)]

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component. [73.26(f)]

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in transportation security plans and should not be used in lieu of performing timely maintenance.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the transportation security program or its elements, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.
[73.26(d)(3)] [73.26(d)(4)] [73.26(e)(1)]

Alternative Measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives. [73.26(a)]

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 11 – Category I – Moderately Dilute: Transportation Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a transportation security program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The transportation security program should be designed to immediately detect attempts to remove Category I - moderately dilute SNM and provide sufficient delay through the use of delay features and armed personnel to allow prompt recovery of SNM by law enforcement agencies.

The transportation security program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness. The program should address the security of the material from the custody transfer time at the point of departure and until the custody transfer time at destination.

In addition to these transportation security requirements, the NRC may require, depending on the individual transport conditions, alternate or additional measures deemed necessary to protect against theft and diversion or sabotage of Category I – moderately dilute SNM.

Licensees should ensure that the design of the transportation security program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the transportation security program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

Licensees should establish, maintain, and implement a performance evaluation program in accordance with Part 73, Appendix B to demonstrate and assess the effectiveness of armed personnel to implement the protective strategy. However, no NRC-conducted force-on-force exercises are required.

Licensees should establish, maintain, and implement an access authorization program and should describe the program in the transportation security plan.

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

Transportation Security Plan

Licensees should develop, maintain and implement an NRC-approved transportation security plan that describes how they will meet the performance objective and physical protection requirements.

Licensees should develop, maintain and follow a Training and Qualification Plan that describes how they will meet the criteria in Part 73, Appendix B.

Licensees should develop, maintain and implement a Safeguards Contingency Plan that describes how they will meet the criteria in Part 73, Appendix C.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the physical protection requirements and security plans.

Security Organization

Licensees or their agents should establish and maintain a transportation security organization that is designed, staffed, trained, qualified and equipped to implement its transportation security program.

The transportation security organization should follow a management system to oversee the transportation security program including having at least one member at the movement control center during the course of any shipment to direct activities.

Members of the security organization including armed escorts, armed response personnel or guards, and a movement control center staff should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties.

Notifications

Licensees or their agents should provide advance notification to the receiver of any planned shipment specifying the mode of transport, estimated time of arrival, and location of the nuclear material transfer point.

Licensees or their agents should receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport.

Licensees or their agents should provide advance notification to NRC in accordance with §73.72.

Licensees or their agents should notify NRC and the receiver of the commencement of the shipment.

Transportation Route

The transportation security plan should include a description of the transportation route, including the location of SNM transfer points, safe havens, and response forces.

Shipments should be scheduled to avoid regular patterns and preplanned to avoid areas of natural disaster, civil disorders, or other security threats. Shipments should be planned in order to minimize the number of material transfers and the storage time, and to assure that deliveries occur at a time when the receiver at the final delivery point is present to accept the shipment.

Arrangements should be made with law enforcement authorities or other response forces along the route of shipments for their response to an emergency or a call for assistance.

Security arrangements for each shipment should be approved by the NRC prior to submitting the seven-day notice required by §73.72. Information to be supplied to the Commission in addition to the general security plan information is as follows:

> Shipper, consignee, carriers, transfer points, modes of shipment, point where escorts will relinquish responsibility or will accept responsibility for the shipment; arrangements made for transfer of shipment security, and security arrangements at points where escorts accept responsibility for an import shipment.

Transportation Security System

Shipments of Category I – moderately dilute SNM should be conducted utilizing transportation security systems including a closed and locked conveyance featuring a specially designed transportation security compartment, SNM containers, secure tiedowns, and physical protection features. However, packages weighing more than 2000 kg may be carried in open vehicles. Such packages should be tied down or securely attached to the vehicle or freight container. The packages should be locked and sealed.

- The transportation security system should provide for immediate detection of attempts to compromise the integrity of the transportation compartment and access SNM containers.
- The transportation security system should provide resistance to and delay of access to Category I – moderately dilute SNM necessary to achieve the performance objectives as stated above.
- The transportation security system should provide for continuous determination of the position of the shipment and communication of the positioning information to the movement control center.

Category I – moderately dilute SNM should be shipped in containers that are protected by tamper-indicating seals. The containers should also be locked if they are not in another locked container or transport. The outermost container or transport should be protected by tamper-indicating seals.

The integrity of locks and seals should be checked before departure, during intermodal transfers, and upon arrival.

For shipment by road, design features of the truck or trailer should permit immobilization of the truck or of the cargo-carrying portion of the vehicle. The cab of the transport vehicle should be bullet-resistant. The transport vehicle should be occupied by at least two individuals one of whom serves as an armed escort. At a minimum, the transport vehicle should be lead and trailed by escort vehicles occupied by at least two armed escorts each. Additionally, a separate lead vehicle with at least two armed response personnel should be conducting route reconnaissance ahead of the transport.

For shipment by air, shipments should be conducted on an exclusive-use cargo aircraft in a secure and locked compartment or container.

For shipment by rail, shipments should be made in a freight train in an exclusive use fully closed and locked conveyance.

For shipment by sea, shipments should be made only on an exclusive-use transport vessel.

Access Controls

Performance capabilities

Licensees should control access to SNM loading and transfer areas, transportation security systems, transport and escort vehicles, aircraft, rail cars, and containers where Category I – moderately dilute material is located as needed to satisfy the general performance objective and requirements.

Licensees should implement a numbered photo identification badge for all individuals who will have custody of a shipment. Badges should be clearly displayed by all individuals.

Prior to transfer, the shipment should only be released when the individual who is in possession of the shipment has assured positive identification of all of the persons assuming custody for the shipment.

Licensees should develop and implement procedures for search of conveyance and escort vehicles prior to loading or transfer. The conveyance and escort vehicles should be searched for explosives, incendiary devices or other items or conditions that have the potential of compromising the shipment. Following the search, the conveyance must remain inside a controlled access area or under continuous surveillance.

Licensees should limit unescorted access to the protected and controlled access areas, transports, escort vehicles, aircraft, rail cars, to only individuals who require unescorted access to perform assigned duties and responsibilities.

Licensees should control all keys, locks, combination, passwords and related access control devices to reduce the probability of compromise.

Movement Control Center

The transportation security program should include a movement control center staffed and equipped to monitor and control Category I – moderately dilute SNM shipments, to communicate with law enforcement authorities, and to respond to safeguards contingencies.

The movement control center should be staffed continuously by at least two individuals who will actively monitor the progress of the shipment with one individual having the authority to coordinate the physical protection activities.

The movement control center personnel must monitor the shipment continuously, i.e., 24-hours per day, from the time the shipment commences, or if delivered to a carrier for transport, from the time of delivery of the shipment to the carrier, until safe delivery of the shipment at its final destination, and must immediately notify the appropriate agencies in the event of a safeguards event under the provisions of § 73.71 of this part. Monitoring should include the use of shipment positioning information and voice communication to maintain information about the shipment's position and status.

The movement control center personnel and the armed escorts must maintain a written log for each shipment, which will include information describing the shipment and significant events that occur during the shipment. The log must be available for review by authorized NRC personnel for a period of at least 3 years following completion of the shipment.

Licensees should limit unescorted access to the movement control center to only individuals who require unescorted access to perform assigned duties and responsibilities. No single adversary action should prevent the movement control center from performing its functions.

Communication

The Category I – moderately dilute SNM conveyance and each escort vehicle should be equipped with redundant communication capabilities that provide 2-way secure communications between the conveyance, the escort vehicle(s), the movement control center, and one another. To ensure that 2-way communication is possible at all times, alternate communications should not be subject to the same failure modes as the primary communication.

Shipment personnel and the movement control center should be equipped with communication abilities that provide communications with law enforcement agencies along the route.

Response

Performance capabilities

Licensees should establish and maintain, at all times, properly trained, qualified and equipped personnel required to respond to attempts of theft and sabotage of nuclear material by detecting and delaying the threat and by communicating relevant information to law enforcement agencies along the route to ensure prompt recovery of nuclear material.

Licensees should ensure that all firearms, ammunition and equipment necessary to implement security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

Licensees should train each armed member of the transportation security organization to prevent or impede acts of theft and diversion and radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law.

Licensees should provide tactical armed response personnel consisting of armed escorts which may be augmented by additional personnel to carry out armed response duties and execute the protective strategy. Licensees should designate an individual who is responsible for directing the tactical response.

The minimum number of LEA armed response personnel available for timely response should be documented. Armed response personnel should have knowledge of features and operations of the transport sufficient for execution of the protective strategy.

Tactical Responders

Licensees should determine the minimum number of tactical response personnel to satisfy the general performance objectives and requirements and implement the protective strategy.

Tactical response team members should be available for immediate response at all times during the transportation of the material and may not be assigned other duties or responsibilities that could interfere with their assigned response duties.

Export and Import Shipments

Licensees who import Category I – moderately dilute SNM should make arrangements to assure that the material will be protected in transit as follows:

- An individual designated by the licensee or his agent, or as specified by a contract of carriage, should confirm the container count and examine locks and/or seals for

evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.

- The shipment should be protected at all times within the geographical limits of the United States as provided in this section and § 73.27. The licensee should retain each required record for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to ship this material, and superseded material for three years after each change.

Licensees who export Category I – moderately dilute SNM should comply with the transportation security requirements, as applicable, up to the first point where the shipment is taken off the transport outside the United States. The licensee should retain each record required by these sections for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to export this material, and superseded material for three years after each change.

Heightened Security

Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.

Security Program Review

The transportation security program should be reviewed at least every 12 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program.

The review should include an audit of transportation security procedures and practices, an evaluation of the effectiveness of the transportation security system, an audit of the transportation security system testing and maintenance program, and an audit of commitments established for response by law enforcement authorities or other response forces.

The results and recommendations of the review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, should be documented in a report to the responsible organization management and to corporate management at least one level higher than that having responsibility for the day-to-day operation.

Maintenance and Testing

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

The maintenance and testing program should be described in transportation security plans.

During installation and construction of physical protection related components, licensees should assure that they comply with their respective design criteria and performance specifications.

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented .

Preoperational tests and inspections should be conducted for physical protection related subsystems and components to demonstrate their effectiveness, availability, and reliability with respect to their respective design criteria and performance specifications.

Operational tests and inspections should be conducted for physical protection related subsystems and components to ensure that they are maintained in an operable and effective condition.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the transportation security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in transportation security plans and should not be used in lieu of performing timely maintenance.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the transportation security program or its elements, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Alternative Measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 12 – Category I – Highly Dilute: Transportation Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a transportation security program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. The transportation security plan may be incorporated into the fixed site security plan as appropriate.

The transportation security program should be designed to detect attempts to remove SNM and notify law enforcement agencies to allow timely recovery of SNM. As appropriate, the program also should be designed to minimize the possibility and manage consequences of radiological sabotage.

The transportation security program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness. The program should address the security of the material from the custody transfer time at the point of departure and until the custody transfer time at destination.

Licensees should ensure that the design of the transportation security program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the transportation security program.
Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program. This program may be incorporated into the fixed site program, as appropriate.

Transportation Security Plan

Licensees should develop, maintain and implement an NRC-approved Transportation Security Plan for transportation of Category I – highly dilute SNM. The transportation security plan should describe how the licensees will meet the performance objective and transportation security requirements.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the transportation security requirements and security plans.

Security Organization

Licensees or their agents should establish and maintain a transportation security organization that is designed, staffed, trained, qualified and equipped to implement its transportation security program. Arrangement for the in-transit physical protection of the material should be made by

1) the shipper unless the receiver is a licensee and has agreed in writing, or 2) the receiver unless the shipper is a licensee and has agreed in writing.

The transportation security organization should follow a management system to oversee the transportation security program.

Members of the security organization should possess knowledge, skills and abilities and be trained and equipped to perform their assigned duties.

Transportation Security Measures

General requirements

Shipments of Category I – highly dilute SNM should be conducted in closed and locked conveyances, compartments or freight containers. However, packages weighing more than 1000 kg that are locked or sealed may be transported in open vehicles. For air transport, Category I – highly dilute SNM should be transported in a cargo aircraft.

Packages should be secured to a vehicle or freight container.

Category I – highly dilute SNM should be shipped in containers that are protected by tamper-indicating seals.

The integrity of locks and seals should be checked before departure and upon arrival.

Each licensee who arranges for the in-transit physical protection of Category I – highly dilute SNM, or who takes delivery of this material free on board (f.o.b.) the point at which it is delivered to a carrier for transport should:

- Arrange for two-way communications between the transport and the licensee or its designee: (A) To periodically confirm the status of the shipment, (B) for notification of any delays in the scheduled shipment, (C) to request appropriate local law enforcement agency response in the event of an emergency, and (D) for prompt notification of the licensee or its designee of attempts of theft or sabotage. Both the transport and the licensee or its designee should be able to contact law enforcement agencies.
- Establish and maintain written response procedures for dealing with threats of thefts or thefts or sabotage of this material. The licensee should retain a copy of the current response procedures as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the original procedures were developed and copies of superseded material must be retained for three years after each change.
- Make arrangements to be notified immediately of the arrival of the shipment at its destination, of any attempts of theft or sabotage, or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination.

- Initiate immediate response by contacting law-enforcement agencies or initiate immediately a trace investigation of any shipment that is determined to be lost or unaccounted for after the estimated arrival time.
- Promptly notify the NRC Operations Center of any attempts of theft or sabotage or the loss of the shipment and within one hour after recovery of or accounting for such lost shipment in accordance with the provisions of §73.71 of this part.

Shipper requirements

Each licensee who transports, exports or delivers to a carrier for transport Category I – highly dilute SNM should:

- Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification,
- Receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport,
- Develop and implement procedures for search of conveyance prior departure from the point of origin or transfer. Following the search, the conveyance must remain inside a controlled access area or under continuous surveillance.
- Prior to transfer, release the shipment only when the individual who is in possession of the shipment has assured positive identification of all of the persons assuming custody for the shipment.

Receiver requirements

Each licensee who receives Category I – highly dilute SNM should:

- Immediately accept the shipment upon arrival,
- Check the integrity of the locks, containers and seals upon receipt of the shipment, and
- Notify the shipper of receipt of the material.

<u>Export and Import Shipments</u>

Licensees who import Category I – highly dilute SNM should make arrangements to assure that the material will be protected in transit as follows:

- An individual designated by the licensee or his agent, or as specified by a contract of carriage, should confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.
- The shipment should be protected at all times within the geographical limits of the United States as provided in this section. The licensee should retain each required record for three years after the close of period for which the licensee possesses the SNM under

each license authorizing the licensee to ship this material, and superseded material for three years after each change.

Licensees who export Category I – highly dilute SNM should comply with the transportation security requirements. The licensee should retain each record required by these sections for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to export this material, and superseded material for three years after each change.

Heightened Security

Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.

Security Program Review

The transportation security program should be reviewed at least every 24 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program.

The review should include an audit of transportation security equipment, procedures and practices.

The results and recommendations of the review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, should be documented in a report to the responsible organization management and to corporate management at least one level higher than that having responsibility for the day-to-day operation.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the transportation security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in transportation security plans and should not be used in lieu of performing timely maintenance.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

Attachment 13 – Category II: Transportation Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a transportation security program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The transportation security program should be designed to immediately detect attempts to remove SNM and provide sufficient delay through the use of delay features and armed personnel to allow prompt recovery of SNM by law enforcement agencies.

The transportation security program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness. The program should address the security of the material from the custody transfer time at the point of departure and until the custody transfer time at destination.

In addition to these transportation security requirements, the NRC may require, depending on the individual transport conditions, alternate or additional measures deemed necessary to protect against theft and diversion or sabotage of Category II SNM.

Licensees should ensure that the design of the transportation security program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the transportation security program, including the ability of armed and unarmed personnel to perform assigned duties and responsibilities required by the security plans and licensee procedures.

Licensees should establish, maintain, and implement a performance evaluation program in accordance with Part 73, Appendix B to demonstrate and assess the effectiveness of the armed personnel in implementing the protective strategy.

Licensees should establish, maintain, and implement an access authorization program and should describe the program in the transportation security plan. [73.67(e)(3)]

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

Transportation Security Plan

Licensees should develop, maintain and implement an NRC-approved transportation security plan that describes how they will meet the performance objective and transportation security requirements.

Licensees should develop, maintain and follow a Training and Qualification Plan that describes how they will meet the criteria in Part 73, Appendix B.

Licensees should develop, maintain and implement a Safeguards Contingency Plan that describes how they will meet the criteria in Part 73, Appendix C.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the transportation security requirements and security plans.

Security Organization

Licensees or their agents should establish and maintain a transportation security organization that is designed, staffed, trained, qualified and equipped to implement its transportation security program.

The transportation security organization should follow a management system to oversee the transportation security program including having at least one member (at the movement control center during the course of any shipment) to direct activities.

Members of the security organization including armed escorts, armed response personnel or guards, and movement control center staff should possess knowledge, skills and abilities and be trained, equipped and qualified to perform their assigned duties.

Notifications

Licensees or their agents should provide advance notification to the receiver of any planned shipment specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification. [73.67(e)(1)]

Licensees or their agents should receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport. [73.67(e)(1)]

Licensees or their agents should provide advance notification to NRC in accordance with §73.72.

Transportation Route

The transportation security plan should include a description of the transportation route, including the location of SNM transfer points, safe havens, and response forces.

Shipments should be scheduled to avoid regular patterns and preplanned to avoid areas of natural disaster, civil disorders, or other security threats. Shipments should be planned in order

to minimize the number of material transfers and the storage time, and to assure that deliveries occur at a time when the receiver is present to accept the shipment. [73.67(e)(1)]

Arrangements should be made with law enforcement authorities or other response forces along the route of shipments for their response to an emergency or a call for assistance.

Security arrangements for each shipment should be approved by the NRC prior to submitting the seven-day notice required by §73.72. Information to be supplied to the Commission in addition to the general security plan information is as follows:

> Shipper, consignee, carriers, transfer points, modes of shipment, point where escorts will relinquish responsibility or will accept responsibility for the shipment, arrangements made for transfer of shipment security, and security arrangements at point where escorts accept responsibility for an import shipment.

Transportation Security System [73.67(e)(4)]

Shipments of Category II SNM should be conducted utilizing transportation security systems including a closed and locked conveyance featuring a specially designed transportation security compartment, SNM containers, secure tiedowns, and physical protection features.

- The transportation security system should provide for immediate detection of attempts to compromise the integrity of the transportation compartment and access SNM containers.
- The transportation security system should provide resistance to and delay of access to Category II SNM necessary to achieve the performance objectives as stated above
- The transportation security system should provide for continuous determination of the position of the shipment and communication of the positioning information to the movement control center.

Category II SNM should be shipped in containers that are protected by tamper-indicating seals. The containers should also be locked if they are not in another locked container or transport. The outermost container or transport should be protected by tamper-indicating seals.

The integrity of locks and seals should be checked before departure, during intermodal transfers, and upon arrival. [73.67(e)(1) & (2)]

For shipment by road, the transport vehicle should be occupied by at least two individuals one of whom serves as an armed escort. At a minimum, the transport vehicle should be lead and trailed by escort vehicles occupied by at least two armed escorts each.

For shipment by air, shipments should be conducted on an exclusive-use cargo aircraft in a secure and locked compartment or container.

For shipment by rail, shipments should be made in a freight train in an exclusive use fully closed and locked conveyance.

For shipment by sea, shipments should be made only on a cargo transport vessel.

Access Controls

Performance capabilities

Licensees should control access to SNM loading and transfer areas, transportation security systems, transport and escort vehicles, aircraft, rail cars, and containers where Category II material is located as needed to satisfy the general performance objective and requirements.

Licensee should establish, maintain, and implement an access authorization program and should describe the program in the transportation security plan. The insider mitigation program should monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to transportation security systems, movement control center, and SNM transfer areas, and implement defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent theft and diversion or radiological sabotage.

Licensees should implement a numbered photo identification badge for all individuals who will have custody of a shipment. Badges should be clearly displayed by all individuals.
Prior to transfer, the shipment should only be released when the individual who is in possession of the shipment has assured positive identification of all of the persons assuming custody for the shipment.

Licensees should develop and implement procedures for search of conveyance and escort vehicles prior to loading or transfer. The conveyance and escort vehicles should be searched for explosives, incendiary devices or other items or conditions that have the potential of compromising the shipment. Following the search, the conveyance must remain inside a controlled access area or under continuous surveillance.

Licensees should limit unescorted access to the protected and controlled access areas, transports, escort vehicles, aircraft, rail cars, to only individuals who require unescorted access to perform assigned duties and responsibilities.

Licensees should control all keys, locks, combination, passwords and related access control devices to reduce the probability of compromise.

Movement Control Center [73.67(e)(3)]

The transportation security program should include a movement control center staffed and equipped to monitor and control Category II SNM shipments, to communicate with law enforcement authorities, and to respond to safeguards contingencies.

The movement control center should be staffed continuously by at least one individual who will actively monitor the progress of the shipment and who has the authority to coordinate the physical protection activities.

The movement control center personnel must monitor the shipment continuously, i.e., 24-hours per day, from the time the shipment commences, or if delivered to a carrier for transport, from the time of delivery of the shipment to the carrier, until safe delivery of the shipment at its final destination, and must immediately notify the appropriate agencies in the event of a safeguards event under the provisions of §73.71 of this part. Monitoring should include the use of shipment positioning information and voice communication to maintain information about the shipment's position and status. [73.67(e)(3)]

The movement control center personnel and the armed escorts must maintain a written log for each shipment, which will include information describing the shipment and significant events that occur during the shipment. The log must be available for review by authorized NRC personnel for a period of at least 3 years following completion of the shipment.

Licensees should limit unescorted access to the movement control center to only individuals who require unescorted access to perform assigned duties and responsibilities. No single adversary action should prevent the movement control center from performing its functions.

Communication [73.67(e)(3)]

The Category II SNM conveyance and each escort vehicle should be equipped with redundant communication abilities that provide 2-way secure communications between the conveyance, the escort vehicle(s), the movement control center, and one another. To ensure that 2-way communication is possible at all times, alternate communications should not be subject to the same failure modes as the primary communication.

Shipment personnel and the movement control center should be equipped with communication abilities that provide communications with law enforcement agencies along the route.

Response

Performance capabilities

Licensees should establish and maintain, at all times, properly trained, qualified and equipped personnel required to respond to attempts of theft and sabotage of nuclear material by detecting and delaying the threat and by communicating relevant information to law enforcement agencies along the route to ensure timely recovery of nuclear material.

Licensees should ensure that all firearms, ammunition and equipment necessary to implement security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

Licensees should train each armed member of the transportation security organization to prevent or impede acts of theft and diversion and radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law.

Licensees should provide tactical armed response personnel consisting of armed escorts which may be augmented by additional personnel to carry out armed response duties and execute the protective strategy. Licensees should designate an individual who is responsible for directing the tactical response.

The minimum number of LEA armed response personnel available for timely response should be documented. Armed response personnel should have knowledge of features and operations of the transport sufficient for execution of the protective strategy.

Tactical Responders

Licensees should determine the minimum number of tactical response personnel to satisfy the general performance objectives and requirements and implement the protective strategy.

Tactical response team members should be available for immediate response at all times during the transportation of the material and may not be assigned other duties or responsibilities that could interfere with their assigned response duties.

Export and Import Shipments [73.67(e)(5) & (6)]

Licensees who import or export Category II SNM should make arrangements to assure that the material will be protected in transit as follows:

- An individual designated by the licensee or his agent, or as specified by a contract of carriage, should confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.
- The shipment should be protected at all times within the geographical limits of the United States as provided in this section and § 73.27. The licensee should retain each required record for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to ship this material, and superseded material for three years after each change.

Licensees who export Category II SNM should comply with the transportation security requirements, as applicable, up to the first point where the shipment is taken off the transport outside the United States. The licensee should retain each record required by these sections for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to export this material, and superseded material for three years after each change.

Heightened Security

Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.

Security Program Review

The transportation security program should be reviewed at least every 12 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program.

The review should include an audit of transportation security procedures and practices, an evaluation of the effectiveness of the transportation security system, an audit of the transportation security system testing and maintenance program, and an audit of commitments established for response by law enforcement authorities.

The results and recommendations of the review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, should be documented in a report to the responsible organization management and to corporate management at least one level higher than that having responsibility for the day-to-day operation.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance, testing and calibration program to ensure that security systems and equipment are tested for operability and performance at predetermined intervals, maintained in operable condition, and are capable of performing their intended functions.

The maintenance and testing program should be described in transportation security plans.

During installation and construction of physical protection related components, licensees should assure that they comply with their respective design criteria and performance specifications.

Implementing procedures should specify operational and technical details required to perform maintenance, testing and calibration activities and criteria for determining when problems, failures, deficiencies or other findings should be documented.

Preoperational tests and inspections should be conducted for physical protection related subsystems and components to demonstrate their effectiveness, availability, and reliability with respect to their respective design criteria and performance specifications.

Operational tests and inspections should be conducted for physical protection related subsystems and components to assure their maintenance in an operable and effective condition.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the transportation security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in transportation security plans and should not be used in lieu of performing timely maintenance.

Records [73.67(e)(4)]

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

If a contracted security force is used to implement the transportation security program or its elements, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Alternative Measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Orders regarding simultaneous shipments [73.67(e)(7)]

If, after receiving advance notice pursuant to § 73.72 from a licensee planning to import, export, transport, deliver to a carrier for transport in a single shipment, or take delivery at the point where it is delivered to a carrier, Category II material, it appears to the Commission that two or more shipments of such material, constituting in the aggregate an amount equal to or greater

than a Category I quantity of SNM, may be in route at the same time, the Commission may order one or more of the shippers to delay shipment according to the following provisions:

The shipper should provide to the Commission, upon request, such additional information regarding a planned shipment as the Commission considers pertinent to the decision on whether to delay such shipment.

The receiver of each shipment, or the shipper if the receiver is not a licensee, should notify the Director, Division of Security Policy, Office of Nuclear Security and Incident Response by telephone, no later than 24 hours after arrival of such shipment at its final destination, or after such shipment has left the United States as an export, to confirm the integrity of the shipment at the time of receipt or exit from the United States.

The Commission should notify the affected shippers no later than two days before the scheduled shipment date that a given shipment is to be delayed.

Attachment 14 – Category II – Moderately Dilute: Transportation Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a transportation security program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The transportation security program should be designed to immediately detect attempts to remove SNM and notify law enforcement agencies to allow prompt recovery of SNM. As appropriate, the program also should be designed to minimize the possibility and manage consequences of radiological sabotage.

The transportation security program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness. The program should address the security of the material from the custody transfer time at the point of departure and until the custody transfer time at destination.

Licensees should ensure that the design of the transportation security program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the transportation security program. [1]

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program. This program may be incorporated into the fixed site program, as appropriate.

Transportation Security Plan

Licensees should develop, maintain and implement a transportation security plan that describes how they will meet the performance objective and transportation security requirements.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the transportation security requirements and security plans.

The transportation security plan may be incorporated into the fixed site security plan as appropriate.

The transportation security plan should include or reference documents including shipment routing information, including location of SNM transfer areas and safe havens. Shipments should be scheduled to avoid areas of natural disaster, civil disorders, or other security threats. Shipments should be planned in order to minimize the number of material transfers and the

storage time, and to assure that deliveries occur at a time when the receiver is present to accept the shipment.

Arrangements should be made with law enforcement authorities or other response forces along the route of shipments for their response to an emergency or a call for assistance.

Security Organization

Licensees or their agents should establish and maintain a transportation security organization that is designed, staffed, trained, qualified and equipped to implement its transportation security program. Arrangement for the in-transit physical protection of the material should be made by 1) the shipper unless the receiver is a licensee and has agreed in writing or 2) the receiver unless the shipper is a licensee and has agreed in writing.

The transportation security organization should follow a management system to oversee the transportation security program including having at least one member to direct activities.

Members of the security organization should possess knowledge, skills and abilities and be trained and equipped to perform their assigned duties.

Access Controls

Access to SNM loading and transfer areas, a conveyance and containers where Category II – moderately dilute material is located should be controlled as needed to satisfy the general performance objective and requirements.

Licensees should implement a numbered photo identification badge program for all individuals who will have custody of a shipment. Badges should be clearly displayed by all individuals.

Licensees should control keys, locks, combination, passwords and related access control devices to satisfy the general performance objective and requirements.

Personnel Trustworthiness

Licensee should establish, maintain, and implement a personnel trustworthiness program and should describe the program in the transportation security plan. The program should monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to SNM transport and SNM transfer areas to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to minimize the possibility of theft and diversion or radiological sabotage.

Transportation Security Measures

General requirements

Shipments of Category II – moderately dilute SNM should be conducted in closed and locked conveyances, compartments or freight containers. However, packages weighing more than 1000 kg that are locked or sealed may be transported in open vehicles. For air transport, Category II – moderately dilute SNM should be transported in a cargo aircraft.

Packages should be secured to a vehicle or freight container.

Category II – moderately dilute SNM should be shipped in containers that are protected by tamper-indicating seals.

The integrity of locks and seals should be checked before departure and upon arrival.

Each licensee who arranges for the in-transit physical protection of Category II – moderately dilute SNM, or who takes delivery of this material free on board (f.o.b.) the point at which it is delivered to a carrier for transport should:

- Designate a point of contact and arrange for two-way communications between the transport and the licensee or its designee: (A) to periodically confirm the status of the shipment (B) for notification of any delays in the scheduled shipment, (C) to request appropriate local law enforcement agency response in the event of an emergency and (D) for prompt notification of the licensee or its designee of attempts of theft or sabotage. Both the transport and the designated point of contact should be able to contact law enforcement agencies.
- Ensure coordination with law enforcement agencies along the route of the shipment.
- Establish and maintain written response procedures for dealing with threats of thefts or thefts or sabotage of this material, transfer of custody, response to abnormal situations (e.g. accidents), reporting, and surveillance of the cargo. The procedures should specify that the conveyance or SNM packages should not be left unattended.
- Make arrangements to be notified immediately of the arrival of the shipment at its destination, of any attempts of theft or sabotage, or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination.
- Initiate immediate response by contacting law-enforcement agencies or initiate immediately a trace investigation of any shipment that is determined to be lost or unaccounted for.
- Promptly notify the NRC Operations Center of any attempts of theft or sabotage or the loss of the shipment and within one hour after recovery of or accounting for such lost shipment in accordance with the provisions of §73.71 of this part.

Each licensee who arranges for the physical protection of Category II – moderately dilute while in transit or who takes delivery of this material free on board (f.o.b.) the point at which it is delivered to a carrier for transport should comply with the requirements of this section. The licensee should retain each required record for three years after close of period licensee

possesses special nuclear material under each license that authorizes these licensee activities. Copies of superseded material must be retained for three years after each change.

Shipper requirements

Each licensee who transports, exports or delivers to a carrier for transport Category II – moderately dilute SNM should:

- Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification,
- Receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport,
- Provide advance notification to NRC in accordance with §73.72,
- Develop and implement procedures for search of conveyance prior to loading or transfer. The conveyance and escort vehicles should be searched for explosives, incendiary devices or other items or conditions that have the potential of compromising the shipment. Following the search, the conveyance must remain inside a controlled access area or under continuous surveillance.
- Prior to transfer, the shipment should only be released when the individual who is in possession of the shipment has assured positive identification of all of the persons assuming custody for the shipment.

Receiver requirements

Each licensee who receives Category II – moderately dilute SNM should:

- Immediately accept the shipment upon arrival,
- Check the integrity of the locks, containers and seals upon receipt of the shipment, and
- Notify the shipper of receipt of the material.

<u>Orders regarding simultaneous shipments</u>

If, after receiving advance notice pursuant to §73.72 from a licensee planning to import, export, transport, deliver to a carrier for transport in a single shipment, or take delivery at the point where it is delivered to a carrier, Category II – moderately dilute material, it appears to the Commission that two or more shipments of such material, constituting in the aggregate an amount equal to or greater than a Category I quantity of SNM, may be in route at the same time, the Commission may order one or more of the shippers to delay shipment according to the following provisions:

- The shipper should provide to the Commission, upon request, such additional information regarding a planned shipment as the Commission considers pertinent to the decision on whether to delay such shipment.

- The receiver of each shipment, or the shipper if the receiver is not a licensee, should notify the Director, Division of Security Policy, Office of Nuclear Security and Incident Response by telephone, no later than 24 hours after arrival of such shipment at its final destination, or after such shipment has left the United States as an export, to confirm the integrity of the shipment at the time of receipt or exit from the United States.

The Commission should notify the affected shippers no later than two days before the scheduled shipment date that a given shipment is to be delayed.

Export and Import Shipments

Licensees who import Category II – moderately dilute SNM should make arrangements to assure that the material will be protected in transit as follows:

- An individual designated by the licensee or his agent, or as specified by a contract of carriage, should confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.
- The shipment should be protected within the geographical limits of the United States as provided in this section. The licensee should retain each required record for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to ship this material, and superseded material for three years after each change.

Licensees who export Category II – moderately dilute SNM should comply with the transportation security requirements. The licensee should retain each record required by these sections for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to export this material, and superseded material for three years after each change.

Heightened Security

Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.

Security Program Review

The transportation security program should be reviewed at least every 24 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program.

The review should include an audit of transportation security procedures and practices, an evaluation of the effectiveness of the transportation security system, and an audit of the transportation security system testing and maintenance program.

The results and recommendations of the review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, should be documented in a report to the responsible organization management and to corporate management at least one level higher than that having responsibility for the day-to-day operation.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the transportation security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in transportation security plans and should not be used in lieu of performing timely maintenance.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

The licensee should retain a copy of the current response procedures as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the original procedures were developed and copies of superseded material must be retained for three years after each change.

If a contracted security force is used to implement the transportation security program or its elements, licensees' written agreement with the contractor should be retained by the licensee as a record for the duration of the contract.

Alternative Measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.

Attachment 15 – Category III: Transportation Physical Protection Measures

General performance objective and requirements

Licensees should establish and maintain a transportation security program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety.

The transportation security program should be designed to detect attempts to remove SNM and notify law enforcement agencies to allow timely recovery of SNM. As appropriate, the program also should be designed to minimize the possibility and manage consequences of radiological sabotage. [73.67(a)(1)]

The transportation security program should provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure its effectiveness. The program should address the security of the material from the custody transfer time at the point of departure and until the custody transfer time at destination.

Licensees should ensure that the design of the transportation security program includes sufficient redundancy and diversity to ensure maintenance of the performance capabilities.

Licensees should, upon request, be able to demonstrate the ability to meet Commission requirements through the implementation of the transportation security program. However, no NRC-conducted force-on-force exercises are required. [1]

Licensees should use a method to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program. This program may be incorporated into the fixed site program, as appropriate.

Transportation Security Plan

Licensees should develop, maintain and implement an NRC-approved transportation security plan for transportation of the following types and quantities:

- For Category III SNM, equal or greater than 200 g plutonium or uranium-233; and
- For Category III SNM, equal or greater than 350 g uranium-235 contained in high enriched uranium; equal or greater than 1 kg uranium-235 in uranium enriched to equal or greater than 10 percent U-235 but less than 20 percent; or equal or greater than 10 kg uranium-235 in uranium enriched to greater than natural but below 10 percent U-235.

The transportation security plan should describe how the licensees will meet the performance objective and transportation security requirements.

The transportation security plan may be incorporated into the fixed site security plan as appropriate.

Licensees should develop a management system to develop, implement, revise and oversee security procedures that implement the transportation security requirements and security plans.

The transportation security requirements are applicable only within areas subject to US Regularity authority.

Security Organization

Licensees or their agents should establish and maintain a transportation security organization that is designed, staffed, trained, qualified and equipped to implement its transportation security program. Arrangement for the in-transit physical protection of the material should be made by 1) the shipper unless the receiver is a licensee and has agreed in writing or 2) the receiver unless the shipper is a licensee and has agreed in writing. [73.67(g)(2)]

The transportation security organization should follow a management system to oversee the transportation security program.

Members of the security organization should possess knowledge, skills and abilities and be trained and equipped to perform their assigned duties.

Transportation Security Measures

General requirements

Shipments of Category III SNM should be conducted in closed and locked conveyances, compartments or freight containers. However, packages weighing more than 1000 kg that are locked or sealed may be transported in open vehicles. For air transport, Category III SNM should be transported in a cargo aircraft. [1]

Packages should be secured to a vehicle or freight container.

Category III SNM should be shipped in containers that are protected by tamper-indicating seals. [73.67(g)(1)]

The integrity of locks and seals should be checked before departure, during intermodal transfers, and upon arrival. [73.67(g)(1) & (2)]

Each licensee who arranges for the in-transit physical protection of Category III SNM, or who takes delivery of this material free on board (f.o.b.) the point at which it is delivered to a carrier for transport should:

- Arrange for two-way communications between the transport and the licensee or its designee: (A) To periodically confirm the status of the shipment, (B) for notification of any delays in the scheduled shipment, (C) to request appropriate local law enforcement agency response in the event of an emergency, and (D) for prompt notification of the

licensee or its designee of attempts of theft or sabotage. Both the transport and the licensee or its designee should be able to contact law enforcement agencies. [1]

- Establish and maintain written response procedures for dealing with threats of thefts or diversion and sabotage of this material. Make arrangements to be notified immediately of the arrival of the shipment at its destination, of any attempts of theft or sabotage, or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination. [73.67(g)(3)]
- Initiate immediate response by contacting law-enforcement agencies or initiate immediately a trace investigation of any shipment that is determined to be lost or unaccounted for after the estimated arrival time. [73.67(g)(3)]
- Promptly notify the NRC Operations Center of any attempts of theft or sabotage or the loss of the shipment and within one hour after recovery of or accounting for such lost shipment in accordance with the provisions of § 73.71 of this part. [73.67(g)(3)]

Shipper requirements

Each licensee who transports, exports or delivers to a carrier for transport Category III SNM should:

- Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification, [73.67(g)(1)]
- Receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport, [73.67(g)(1)]
- Develop and implement procedures for search of conveyance prior departure from the point of origin or transfer. Following the search, the conveyance must remain inside a controlled access area or under continuous surveillance. [1]
- Prior to transfer, release the shipment only when the individual who is in possession of the shipment has assured positive identification of all of the persons assuming custody for the shipment. [1]

Receiver requirements

Each licensee who receives Category III SNM should: [73.67(g)(2)]

- Immediately accept the shipment upon arrival,
- Check the integrity of the locks, containers and seals upon receipt of the shipment, and
- Notify the shipper of receipt of the material.

<u>Export and Import Shipments</u>

Licensees who import Category III SNM should make arrangements to assure that the material will be protected in transit as follows:

- An individual designated by the licensee or his agent, or as specified by a contract of carriage, should confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.
- The shipment should be protected within the geographical limits of the United States as provided in this section. The licensee should retain each required record for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to ship this material, and superseded material for three years after each change.

Licensees who export Category III SNM should comply with the transportation security requirements. In this section for the domestic portion of the shipment, the licensee should retain each record required by these sections for three years after the close of period for which the licensee possesses the SNM under each license authorizing the licensee to export this material, and superseded material for three years after each change. [73.67(g)(4)]

Heightened Security

Upon notification by an authorized NRC representative, licensees should implement the specific protective measures based on the threat, which may include postponing a shipment or diverting a shipment to a safe haven location.

Security Program Review

The transportation security program should be reviewed at least every 24 months by individuals independent of both security program management and personnel who have direct responsibility for implementation of the security program.

The review should include an audit of transportation security equipment, procedures and practices.

The results and recommendations of the review, management's findings on whether the transportation security program is currently effective, and any actions taken as a result of recommendations from prior reviews, should be documented in a report to the responsible organization management and to corporate management at least one level higher than that having responsibility for the day-to-day operation.

Compensatory Measures

Licensees should identify criteria and measures to compensate for degraded or inoperable equipment, systems and components of the transportation security program.

Compensatory measures should provide a level of protection that is equivalent to the protection that was provided by the degraded or inoperable equipment, system or component.

Compensatory measures should be implemented with specific time frames necessary to meet the general performance objective and requirements and described in transportation security plans and should not be used in lieu of performing timely maintenance.

Records

The NRC may inspect, copy, and retain copies of all reports, records, and documents required to be kept by regulations, orders, or license conditions, whether the reports, records, and documents are kept by the licensee or a contractor.

The licensee should retain a copy of the current response procedures as a record for three years after the close of period for which the licensee possesses the special nuclear material under each license for which the original procedures were developed and copies of superseded material must be retained for three years after each change.

Licensees should maintain all records required to be kept by regulations, orders, or license conditions, until the NRC terminates the license for which the records were developed, and should maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified.

Alternative Measures

The NRC may authorize applicants or licensees to provide an alternative measure other than ones required in the regulations, if applicants or licensees demonstrate that the alternative measure meets the same performance objectives.

Licensees should submit proposed alternative measure(s) to the NRC for review and approval.

In addition to fully describing the desired changes, licensees should submit a technical basis for each proposed alternative measure. The basis should include an analysis or assessment that demonstrates how the proposed alternative measure provides a level of protection that is at least equal to that which would otherwise be provided by the specific requirement.