Rulemaking for Enhanced Security at Fuel Cycle Facilities; Special Nuclear Material Transportations; Security Force Fatigue at Nuclear Facilities

RIN number: 3150-AJ41

NRC Docket ID: NRC-2014-0118

Regulatory Basis Document – Draft for Public Comment

May 2014

Table of Contents

DRAFT FOR PUBLIC COMMENT
REGULATORY BASIS FOR RULEMAKING TO
ENHANCED SECURITY AT FUEL CYCLE FACILITIES
SPECIAL NUCLEAR MATERIAL TRANSPORTATION SECURITY
SECURITY-FORCE FATIGUE AT NUCLEAR FACILITIES

1. 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:

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

These objectives are discussed in greater detail in Section 3.

This regulatory-basis document encompasses three separate rulemaking efforts:

(1) Enhanced Security at Fuel Cycle Facilities
(2) Special Nuclear Material Transportation Security
(3) Security-Force Fatigue at Nuclear Facilities

In 2006, the Commission approved the staff's schedules and resources for the Enhanced Security at Fuel Cycle Facilities rulemaking effort (NRC, 2006a). Subsequently, 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.

The third rulemaking effort relates to security-force fatigue at fuel cycle facilities. As discussed further in Section 3 and Attachment 2, because of issues being identified at nuclear power reactors, the NRC issued rules regarding work hours for security officers and others at nuclear power reactors. Staff believed that fatigue-related requirements were necessary for the security officers at other licensed facilities also, and staff proposed in COMSECY-04-0037, "Fitness-for-Duty Orders to Address Fatigue of Nuclear Facility Security Force Personnel" (NRC, 2004a), that the Commission issue orders for fatigue-management requirements for a number of classes of material licensees similar to those required at nuclear power reactors. The Commission directed staff in SRM-COMSECY-04-0037 (NRC, 2004c) to use the rulemaking process rather than issuing orders for those materials facilities for which the staff believes fatigue-related requirements are necessary for appropriate personnel. Staff considers it appropriate to include the third rulemaking effort in parallel with the first two, at least during the

development of the regulatory basis, because: (1) the same group of stakeholders have been involved with both rules during outreach and regulatory-basis development, and (2) consolidation and development of the regulatory basis would capitalize on efficiencies gained from the development of one regulatory basis versus two in an environment with limited resources/flat budgets.

Staff is using a phased approach, through rulemaking, to determine which classes of material licensees should fall under the 10 CFR Part 26, "Fitness for Duty Programs," requirements for fatigue-management/work-hour controls. This phased approach uses NRC funds and resources efficiently by examining fatigue-management requirements (work-hour controls) for certain material licensees at this time and within the scope of SRM-COMSECY-04-0037 (NRC, 2004c). As such, this regulatory basis assesses and evaluates the application of fatigue management requirements on security-officer fatigue for Category I, II and III SNM facilities. Consideration of fatigue requirements for other classes of material licensees would be conducted in separate efforts and is outside the scope of this regulatory basis.

The scope of this regulatory basis includes physical protection of SNM at fuel cycle facilities and 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.

The scope of this regulatory basis does not include physical protection of SNM at nuclear power reactors, when covered by §73.55. The nuclear power reactor security regulations were amended in 2009 to include requirements which were imposed by security orders. The robust physical protection at nuclear power reactors using low enriched uranium fuel, that is designed to protect against radiological sabotage, is generally sufficient to provide protection against SNM theft and diversion.

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 are the subject of separate NRC rulemakings and thus are not within the scope of this Regulatory Basis.

The scope of the rulemaking effort 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 in regulating licensees with digital assets. In 2009, the NRC issued a new regulation (i.e., 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, 2012c) 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. The Commission directed staff to gather additional information, conduct stakeholder outreach, and develop recommendations and measures necessary to constitute an adequate chemical security framework at these facilities. Therefore, these 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 2008 to amend 10 CFR 73.37, "Requirements for Physical Protection of Irradiated Reactor Fuel in Transit."

This draft regulatory basis (1) explains why the existing regulations or policies are in need of enhancement, are considered to be outdated, or need to be changed; (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.

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 the needed perspective as to why the various changes and new information, presented in Section 3, 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

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

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 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 special nuclear material, 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 patrols 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 power reactors and Category I facilities), and 10 CFR 73.60, "Additional Requirements for the Physical Protection of Special Nuclear Material at Fixed Sites" (which applied only to Category I facilities). 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). Note that, 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 (DBT) requirements (previously for protecting 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 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 Statements of Consideration. 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 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 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 significance), and in some cases the provisions of a revised 10 CFR 73.60 (for those non-power reactor facilities possessing formula quantities of special nuclear material not meeting the 100 rem per hour self-protection exemption). Application of the requirements of these amendments to non-power

reactors possessing formula quantities of special nuclear material which cannot meet the 100 rem per hour self-protection 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, 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 NRC staff recommendation was not approved by the Commission (48 FR 34056; July 27, 1983). In 1993, §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 as the Upgrade Rule, 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, those 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 (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[2] (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.

c. Although nuclear materials might be involved in a threat to the public through a dispersion scenario, such as by sabotage, SECY-77-79 (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.

---

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

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, 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 and that which 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 matrix) 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 under license. 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 the 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., §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, 10 CFR 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

(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) special nuclear material 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, §73.67(d) and (f) except 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 Category II and III facilities 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 risk of the material being used for malevolent purposes, with physical protection requirements for Category I facilities being more robust than those at Category II facilities, which are more robust than those at Category III facilities. 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. 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 10 CFR 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 NRC 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 agreement 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 special nuclear material 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 a 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.

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 under 10 CFR 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 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," and certificate of compliance holders under 10 CFR Part 76, "Certification of Gaseous Diffusion Plants." Part 26 does not apply to either spent fuel storage facility licensees or non-power reactor licensees who possess, use, or transport formula quantities of irradiated strategic SNM.

3. Regulatory Problem

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

3.1 Consistency

The first objective of this rulemaking is to improve regulatory consistency and clarity. Legislative and policy changes, inconsistencies in the use of terms, the level of detail provided for similar

regulatory requirements, and inconsistencies in 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 NRC 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) and fitness for duty programs (Part 26). 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) 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 a regulatory requirement.

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 regulations are, for the most part, prescriptive and deterministic.

Ensuring consistency in the use of terms for similar security concepts throughout 10 CFR 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 10 CFR 73.55 (74 FR 13926; March 27, 2009) to include making generally applicable the security-order requirements issued to 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," to 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. The new power reactor training and qualification plan requirements in Section VI are essentially the same as the existing Category 1 training and qualification requirements in Sections I through V except for a limited number of differences. However, Sections I through V give greater prescriptive specificity on weapons and equipment. Furthermore, Section VI power reactor requirements, in addition to being more performance-based, contains additional requirements that include contingency drills, a Performance Evaluation Program, and an annual written exam. 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.

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 that 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 has additional requirements specific for Category I materials which are different than those in §73.46. Also, the Power Reactor Security rule in §73.55 includes a subsection (i.e., §73.55(l)) which provides additional physical protection requirements for unirradiated mixed-oxide fuel assembles containing a Category I quantity of plutonium dioxide at power reactors. These requirements and others for power reactor security, while protecting the unirradiated 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.

3.2 Generic Applicability of Security Orders

The second 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[3] 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 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

---

[3] 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.

(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 order to address the new threat environment. However, in SRM-COMSECY-05-0058 (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 Category II fuel cycle facilities 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, 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 (CALs). 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 CALs rather than issuing security orders. The CALs 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 (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 for unescorted access to material at fuel cycle facilities and non-power reactors. Category III fuel cycle facilities 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). Therefore, Category III fuel cycle facilities (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 nuclear power reactors and non-power reactors in §73.57 and for radioactive material in Subpart B, "Background Investigations and Access Control Program," of 10 CFR Part 37, "Physical Protection of Byproduct material."

3.3 Risk Insights

The third objective of this rulemaking is to consider risk insights and operating 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), significant changes in the regulated material and facilities have occurred. For example, the NRC currently regulates gas centrifuge enrichment facilities; and the NRC has licensed a mixed-oxide fuel (containing both uranium and plutonium) fabrication facility and a laser enrichment facility. The NRC has also received an application for a medical isotope production facility 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 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.

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. These include requirements for work-hour controls for security officers at fuel cycle facilities and for safety/safeguards interfaces. 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 new proposed requirement for an insider risk assessment for Category I SNM facilities benefits both physical protection and MC&A goals. Staff also considered the need for new physical protection requirements based on operational 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 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) 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 and low strategic significance are not always interchangeable in practice. Some of the chemical and physical forms of SNM represent less risk than others, even though the materials might fall into the same category. The existing regulations make no distinction based on material attractiveness and impose the same physical protection measures on the two highly different forms of SNM. For materials of low attractiveness, the regulations are 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 a terrorist adversary would have greater difficulty stealing a bulky and heavy item weighing several hundred kilograms. The adversary also would 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.

The exemption approach has been appropriate because of the relatively low risk-significance of highly dilute HEU waste. However, it has significant drawbacks, including the inconsistency of physical protection measures, lack of regulatory stability, and significant resource implications for both licensees and the NRC.

Since the late 1970s, understanding of the technical and security aspects associated with SNM theft scenarios has improved. 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 the following: (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 lead the staff to assess the current regulatory approach to SNM categorization and attractiveness for NRC licensees.

As a result, the NRC has 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. Staff notes that the assumptions related to adversary characteristics and capabilities and to the scenarios discussed in Section 2.1 have evolved; therefore, adversary characteristics and capabilities, and scenarios considered in the study, might vary from the information in Section 2.1.

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 a new material categorization. As part of the proposed rulemaking and as discussed further in Section 4, 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 (weight percent of the 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 Attachment 1.

Threshold Dose-Rate Limit

As discussed in Section 2, 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 unirradiated 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, the existing external radiation dose-rate threshold was considered sufficient to act as an effective deterrent to the unauthorized removal of material. Using external radiation as a security feature is often termed as "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, staff concludes that the external radiation dose-rate in the existing regulations is not sufficient for use as a security feature.

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, 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 Part 73 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 Part 37, 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.

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. 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 studied extensively 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 risk 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 (other than for power reactors) 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)). The classified Sandia National Laboratory (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 studies indicate that smaller quantities of SNM (predominately plutonium) 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.

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 rationalized 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 unirradiated HEU nor LEU are considered a sabotage target. Also, although commercial light-water spent nuclear fuel is less attractive as a source of SNM for an IND, its highly radioactive fission products make it attractive as a potential radiological sabotage target for adversaries and these materials are required to be protected to a degree consistent with §73.51 and §73.55. In addition, the existing physical protection requirements against sabotage for non-power reactors (i.e., §73.60(f)) adequately consider sabotage risk at those facilities.

In 2013, the NRC issued the regulations in 10 CFR Part 37 to establish physical protection requirements for the use and transport of Category 1 and Category 2 quantities of radioactive

---

[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)

material that are widely used in the United States 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.

Fitness for Duty

As discussed above, the NRC issued several security orders to licensees following the terrorist attacks of September 11, 2001, that called for enhanced security. To meet the requirements of these orders, licensees increased the hours worked by their existing security officers. The NRC became aware that security officers at nuclear power reactors were working a large number of hours to meet the order requirements issued to this group (see http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/). Further, licensees needed additional time to complete the hiring and training of the additional security officers necessary to reduce the burden on security officers' work hours. Consequently, on April 29, 2003, the Commission issued Order EA-03-038 (NRC, 2003) requiring compensatory measures related to fitness-for-duty (fatigue) enhancements for security officers at nuclear power reactors, including work-hour limits to address cumulative fatigue from prolonged periods of extended work hours (see http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/). In 2008, the NRC amended Part 26 to include in part fatigue management provisions as well as the compensatory measures from the security orders issued to nuclear power reactors.

Many studies have shown that fatigue impairs human alertness and performance (Akerstedt, 2003, 2007; Banks and Dinges, 2007, 2011; Durmer and Dinges, 2005; Lamond and Dawson, 1999; Monk and Carrier, 2003; Van Dongen et al., 2003). The lack of rest and adequate days off from work, extended work hours, and rotating shifts can result in a cumulative sleep debt (i.e., the difference between the amount of sleep an individual needs and the amount of sleep that individual actually obtains) and performance impairment (Belenky et al., 2003; Dinges et al., 1997; Van Dongen et al., 2003). Studies across various industries have shown that fatigue-induced personnel impairment can increase human error probabilities by factors of more than two to three (Dawson and Reid, 1997; Pilcher and Huffcutt, 1996; Williamson and Feyer, 2000). Fatigue reduces an individual's ability to remain alert, process complex information, and correctly grasp a complex set of circumstances. Fatigue adversely affects memory, slows responses, and increases lapses and incorrect responses (Belenky et al., 2003; Horne, 1988; Williamson et al., 2011). Successful completion of the cognitive and behavioral tasks performed by fuel cycle facility security officers to deter, prevent, and respond to malicious threats, which are important to the protection of public health and safety and the common defense and security, depends on the ability of these personnel to sustain attention, analyze problems, make rapid and accurate decisions, and communicate and work effectively as a team. The ability to perform these cognitive and behavioral tasks is adversely affected by fatigue: sleep-deprived/fatigued workers have difficulty appropriately allocating attention, setting task priorities, and probing or questioning potentially faulty information, and might fail to respond appropriately to emerging events/actions (Durmer and Dinges, 2005; Lamond and Dawson, 1999; Pilcher and Huffcutt, 1996). Fatigued personnel tend to choose riskier strategies and exert less decision making effort than those who are well rested (Harrison and Horne, 2000; Horne, 1988). As can be demonstrated by personnel working many extended shifts in succession, the more severe the fatigue, the greater the adverse effect on alertness, attention, and decision making (Hockey, 1970; Krueger, 1989; Lorist et al., 2000; Totterdell et

al., 1995). Attachment 2 provides additional information about fatigue in general and staff analysis of fatigue issues at fuel cycle facilities.

The staff also investigated and considered how other industries combat fatigue via program that controls work hours of personnel. The staff reviewed other government agencies and found the following information (not all inclusive):

1. Department of the Army Field Manual 6.22-5 (2009) discusses guidelines associated with fatigue and rest. Other documents related to this issue are found in the U.S. Army Training and Doctrine Command Regulation 350-6.

2. U.S. Department of Energy fatigue guidelines (DOE Order 473.3) for protective force (PF) personnel state that PF schedules should be based on: (1) No more than 12 total hours/day, excluding shift change/equipment issuing activities; and (2) No more than 60 hours/week, excluding shift change/equipment issuing activities.

3. Transportation Security Administration (TSA) has guidelines in place for its officers in TSA Management Directive No. 1100-33-1: This is focused on ensuring the fitness of officers for performing their duties, and ensuring that officers are not impaired from the influence of fatigue (sleep deprivation), alcohol, illegals drugs and the misuse or abuse of prescription medication. There are no specific work hour limits referenced.

4. U.S. Department of Transportation (DOT) imposes work hour controls and rest break and scheduling requirements on the entities it regulates across the various modes of transportation, with a focus on vehicle operators. It also imposes fatigue management requirements on other job categories that include safety-related responsibilities (e.g., air traffic controllers and flight crew members), commercial motor vehicle operators and railroad operators. Specific fatigue and work hour requirements can be found in Titles 14, 23, and 49 of the CFR. For example for air traffic controllers, 14 CFR 65.47 establishes the maximum hours for air traffic controllers:

   > Except in an emergency, a certificated air traffic control tower operator must be relieved of all duties for at least 24 consecutive hours at least once during each 7 consecutive days. Such an operator may not serve or be required to serve-:
   > - For more than 10 consecutive hours; or
   > - For more than 10 hours during a period of 24 consecutive hours, unless he has had a rest period of at least 8 hours at or before the end of the 10 hours of duty

In its consideration of the need for fatigue management for security officers at Category I, II, and III facilities, staff collected data from fuel cycle facilities to gauge the extent to which security officers might be working potentially excessive hours. The data is limited in that it represents a snapshot in time and was collected from a subset of facilities. As discussed in Attachment 2, most Category I, II and III licensees appear to control the work hours of their security officers reasonably well. However, the limited data in Attachment 2 shows that at some of the fuel cycle facilities, security personnel might be working schedules with elevated overtime, that may lead to acute and cumulative fatigue[6].

More significantly, the staff collected and reviewed incidents or concerns associated with security officers being either fatigued or inattentive. More significantly, the staff collected and

[6] These terms are explained in Attachment 2

reviewed incidents or concerns associated with security officers being either fatigued or inattentive. Over the past few years, multiple concerns have been raised related to security officer overtime, fatigue or inattentiveness at Category I facilities. For example:

- In April 2012, a concern was raised noting that security officers were working large amounts of overtime for quite a while.

- In August 2013, NRC inspectors observed a security officer who appeared to be inattentive at a check point; the licensee's investigation was unable to determine if the individual was inattentive. The security plan's effectiveness was not decreased because of the check point staffing.

- In October 2013, a concern was raised noting that security officers were working large amounts of overtime.

- In December 2013, a concern was raised noting that security officers were working large amounts of overtime and were fatigued.

The specific cases referenced above were evaluated by either the licensee or NRC inspectors, and no regulatory actions were taken or deemed necessary. In addition, during routine inspections, NRC inspectors monitor security force readiness and have not identified regulatory issues that reduced the effectiveness of the security plan.

In its consideration of the need for fatigue management for security officers at Category I, II, and III facilities, staff is also considering a variety of potential malicious uses and the potential consequences from such malicious uses. Because of similar or possibly greater threats, potential consequences resulting from malicious use of Category I material could be equal to or greater than those posed by nuclear power reactors. The malicious use of Category II and III material would be expected to have consequences less than those posed by a nuclear power reactor. Additionally in evaluating the need for fatigue management for officers at certain fuel cycle facilities, staff considered the role and function of security officers in meeting proposed protective strategies (see Section 4) for the different categories of SNM. For example, Category I security officers perform duties similar to those performed at nuclear power reactors, and security officers at nuclear power reactors are subject to work hour controls in Part 26, Subpart I.

Security officers at Category I, II, and III facilities are part of a physical protection system that integrates people, procedures, and equipment to protect NRC-licensed facilities against adversaries that are intent on performing malicious acts. Security officers at Category I facilities perform job duties that include defending against a DBT. To accomplish this, security officers at Category I facilities are required by regulations to interdict during a malicious event, interpose themselves between adversaries and their targets, and neutralize adversaries through the use of force, including deadly force. Security officers at Category I facilities are subjected to conditions and duties that contribute to fatigue. Security officers' work typically requires high vigilance and situational awareness in work environments that create or exacerbate the effects of fatigue such as rotating 24-hour-coverage shift schedules (that frequently require work during periods of low circadian alertness and impair recovery) and long periods of working alone with low levels of physical activity, social interaction, and limited task diversity.

Based on the above and on Attachment 2, fatigue has the potential to degrade the ability of security officers at Category I facilities to safely and competently perform their duties and might impact public health and safety and the common defense and security. The management of fatigue is necessary to provide high assurance that security officers are capable of communicating; analyzing/processing complex information; making rapid/accurate decisions; and ensuring security can initiate a timely response and interdict an external threat that may require the security officer to use deadly force. It is necessary to fulfill their regulatory obligation to prevent adversaries from acquiring material at Category I facilities to use in an IND. It is a fundamental requirement that implementation of the Commission's security requirements is accomplished by persons who are fit for duty and not impaired by the lack of sleep.

Given the potential for significant consequences associated with malicious use of Category I SNM, and the duties and responsibilities of Category I security officers in protecting such material, the staff concludes that work hour controls should be imposed on these individuals. This conclusion is bolstered by staff's assessment of work hours data in Attachment 2 and reported incidents and concerns.

On the other hand, security officers at Category II and III facilities are not required to interdict adversaries, interpose themselves between adversaries and their targets, or neutralize adversaries. Rather, these security officers are required to delay adversaries and communicate with authorities while local law enforcement performs interdiction and neutralization. Therefore, the staff concludes that security officers at these facilities should not be subject to work hour controls given the consequences associated with the materials at these facilities and the function of the security officers.

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 power reactor licensees must evaluate the safety/security interface under the requirements in 10 CFR 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 International Atomic Energy Agency 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 material control and accounting is to (1) maintain current knowledge of the location of SNM and resolve any discrepancies; (2) prevent undetected access resulting in unauthorized changes to values of SNM at a site that might ultimately result in diversion of SNM; and (3) meet international treaty obligations by accounting for SNM and reporting values. 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 an adequate 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 required 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 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 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, staff believes that it is appropriate to adopt requirements similar to those of §73.58 (applicable to power reactor licensees) for fuel cycle facility licensees. Additionally, 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 10 CFR 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.

Therefore, 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.

Operating Experience

Operating experience derived from nuclear fuel cycle facilities and non-power reactors 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. Operating experience has shown 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 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, operating experience has shown that in some cases Part 50 licensees have stored and possessed Category II or III materials in the owner-controlled area of power reactors, and 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 power reactor.

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 within a 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.

Operating experience has 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.

Operating experience has identified requirements that are imposed by other organizations that should be considered in the physical protection of SNM during transport. The existing NRC SNM transportation security requirements are also 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).

In addition, transportation security technologies and practices have been rapidly advancing during the past 10 to 15 years. Global Positioning System tracking, cell-phone communications, and other modern technologies are now critical to transportation security. Additionally, based on lessons learned 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.

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. 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 but were not limited to: 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.

3.4 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. In a way similar to the approach used in the Power Reactor Security Rule (74 FR 13926; March 27, 2009), 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 without specific direction regarding 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, 2012b). 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. 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 problem. 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 requirements to enhance physical protection based on security orders, risk insights, and lessons learned since 1979.

Changing from a combination of physical protection requirements for three categories and also 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. **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 regarding material attractiveness, **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 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 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, elevated 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 is provided in a non-public attachment to this document (Attachment 1).

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, 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.

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 the early outreach activities, the staff modified the proposed approach. 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. Dilution (concentration) is expressed in weight percent for solids (e.g., weight of uranium-235 divided by the total weight of the SNM material, including non-SNM materials which are not mechanically separable from the SNM) and volumetric concentration for liquids (e.g., grams of SNM per liter of solution).[7] The level of dilution generally corresponds to the difficulty of acquiring and processing SNM. In addition, dilution is one of the factors identified in INFCIRC/225, Revision 5 (IAEA, 2011). 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 SNM concentration equal to or greater than 20 weight percent. Non-dilute materials include, for example, highly attractive HEU, uranium-233, and plutonium metals and compounds.

2. Moderately dilute SNM is defined as material with SNM concentration equal to or greater than 1 weight percent but less than 20 weight percent. 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 SNM concentration less than 1 percent. HEU-contaminated processing waste, for which the recovery of SNM is uneconomic, is an example of highly dilute materials.

The overall proposed material categorization and attractiveness approach then relies on the three defined material attractiveness levels overlaid on the existing NRC material categorization table (Table 4-2). For each pairing of material category and attractiveness, the staff defined an appropriate protective strategy. For example, for non-dilute Category I material, the strategy calls for the protection of the SNM against theft or diversion DBT of §73.1. In contrast, the protection requirements for highly dilute Category I 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.

---

[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.

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.

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

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	≥ 1 5 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

4.2 Fixed Site Physical Protection Changes

Following the proposed changes discussed in Section 4.1, **staff proposes to add three new sets of physical protection requirements** (i.e., for moderately dilute Category I, highly dilute Category I, and moderately dilute Category II) to the existing three sets of physical protection requirements (i.e., Category I (now non-dilute Category I), Category II (now non-dilute Category II) and Category III). Staff further proposes to change those existing physical protection requirements based on security orders, risk insights, and lessons learned. As such, **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.

Staff used the LANL study to develop protective strategies for each SNM Category and material attractiveness level. Staff then determined conceptual physical protection actions that would be needed to support each protective strategy. To improve consistency and clarity and to use a performance-based approach, the NRC staff proposes to have the new regulatory requirements, as appropriate, be consistent with those developed for the Power Reactor Security Rule (74 FR 13926; March 27, 2009). Restructuring the existing requirements similar to those 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. Considering the existing physical protection requirements and those imposed by security orders, staff subsequently developed a set of physical protection requirements for each pairing of SNM Category and material attractiveness.

In general, the actions required by the new requirements for Category I and Category III facilities are not significantly different from what licensees are currently doing to incorporate security-order requirements (discussed in Section 3.2). Because the NRC did not issue Category II security orders to address the new threat environment and the number of Category II licensees is limited, there is a significant difference in existing Category II requirements and the proposed requirements.

The new proposed requirements for theft or diversion of SNM at fixed sites for each category and attractiveness are presented in Attachments 3 through 8. The new proposed requirements 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 new proposed requirements. In addition, proposed requirements developed with consideration of risk insights are noted with a “1” and proposed requirements developed with consideration of security orders are noted with a “2”.

The following subsection further discusses how the regulatory problems presented in Section 3 are addressed by the new proposed requirements.

Orders for Interim Compensatory Measures and Additional Security Measures

As discussed in Sections 1 and 3, 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) 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 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 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.

After a final rule is issued, the agency's long-term objective is to rescind these security orders if all of the requirements are incorporated in the rule or to relax portions of these security orders if only a portion of the security order is addressed by the rule. Some requirements of the security orders, because of their sensitive nature, would continue to be carried out by security order or included in Classified Regulatory Guidance.

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. **Staff proposes six sets of requirements for fixed sites (i.e., for non-dilute Category I, moderately dilute Category I, highly dilute Category I, non-dilute Category II, moderately dilute Category II, 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 as non-dilute.

While the protective strategies and physical protection requirements are similar between some of the new more dilute categories and the non-dilute categories (e.g., between moderately dilute Category I and non-dilute Category II), staff is proposing to keep the sets of physical requirements separate. This will allow greater regulatory flexibility in the future to adjust the physical protection requirements 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 new proposed requirements 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, **staff proposes to require that in order to use the physical protection requirements for dilute materials, the SNM must 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 operating experience discussed in Section 3, staff is proposing several new or modified requirements. These include:

1. **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.** 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. In addition, such language would allow the NRC to impose classified requirements for certain types and quantities of Category I SNM or to place maximum possession limits as license conditions if appropriate.

2. **Staff proposes to require Category I facilities 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.

3. **Staff proposes to require Category I facilities to follow the training and qualification requirements of Section VI of Appendix B to Part 73.** The proposed rule should consider that other facilities cite parts of Sections I through V of Appendix B to Part 73 and unused portions should be removed and reserved. The training and qualification plan requirements in Appendix B to Part 73 were revised into a new Section VI as part of the Power Reactor Security Rule to be more performance-based and to include additional requirements such as performance testing, contingency equipment, and weapons which were contained in security orders.

4. **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. Staff reviewed the proposed requirements and determined that the protection provided in §73.55 for low-enriched uranium fuel meets or exceeds those proposed in Attachment 4.

In keeping with moving towards a material-based approach rather than a mixture of material-based and facility-based requirements, **staff proposes to eliminate §73.60**. The composition of non-power reactor fuel varies. While some non-power reactors use HEU (and others use uranium enriched below 20 percent), the uranium-235 is diluted with other materials in the fuel matrix. As such, non-power reactor fuel would in general be protected as moderately dilute Category II. Staff considers this level of protection to be appropriate for those facilities.

Staff proposes to change the exception in §73.67 for Part 50 licensees to except SNM within the protected area of facilities meeting the requirements of §73.55.

For Part 73, **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 *moderately-dilute special nuclear material* means the material with a special nuclear material concentration of equal to or greater than one weight percent, but less than 20 weight percent for solids and <1 gram per liter for solutions.

- Add *highly-dilute special nuclear material* means the material with a special nuclear material concentration of less than one weight percent for solids and ≥1 gram per liter and <25 gram per liter for 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.

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

Table 4-3: Summary of Fixed Site Proposed Requirements

	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 and 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 local law enforcement agencies to allow recovery of SNM	– Timely detect attempts to remove of SNM and notify LLEA to recovery 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 – Part 26 – including Subpart I	– Implement Program – Management System	– Implement Program – Management System	– Implement Program – Management System
Physical Barrier	– Owner Controlled Area – Vehicle Barrier System/blast analysis – Isolation Zone – Protected Area – Vital Area – Material Access Area – Locked Processes – Vault – Hardened 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 Program	– Protected Area & Controlled Access Area Access Portals – Limit unescorted access – Access Authorization Program per §73.57, §73.59, §73.61 – Controlled Badge Program	– Controlled Access Area Access Portals – Limit unescorted access – Access Authorization Program per §73.57, §73.59, §73.61 – Controlled Badge Program	– Controlled Access Area Access Portals – Limit unescorted access – Controlled Badge Program – Escort Requirements

	– Escort Requirements	– Escort Requirements	– 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 – Secondary Alarm Station (on-site or off-site) – 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/SAS 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	– Deadly Force – Armed Security Officers – LLEA Liaison	– LLEA Liaison – Heightened	– LLEA Liaison

	Officers – LLEA Liaison – Heightened Security	– Heightened Security	Security	
Security Program Review	– Annually – Management Review – CAP or event log – Performance evaluation program	– Bi-annually – Management Review – CAP or event log	– Bi-annually – Management Review – CAP or event log	– Bi-annually – Management Review – CAP or event log
Maintenance & Testing	– Required	– Required	– Required	– None
Compensatory Measures	– In 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, the understanding of consequences associated with sabotage has evolved since the 1970s as well as the threat environment following the events of 9/11. Considering relevant national laboratory studies and the level of protection suggested for theft or diversion (discussed above), 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 of radioactive material (which includes plutonium sealed sources) in Part 37. These additional protection requirements are provided in Attachment 3.

Spent nuclear fuel[8] also poses sabotage risk. The existing regulations use an external radiation dose-rate threshold to, in part, differentiate irradiated and unirradiated materials. As discussed below, staff is proposing to eliminate this external radiation dose-rate threshold. Moreover, the physical protection of spent nuclear fuel is provided in §73.51(see discussion in Section 2), and §72.180, "Physical Protection Plan." As such to reduce confusion of whether spent nuclear fuel should be protected in accordance with §73.50 or other regulations, **staff is proposing to eliminate the requirements in §73.50.** 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. Staff proposes to also apply the additional protection requirements in Attachment 10 to quantities of spent nuclear fuel less than 100 grams. Quantities of spent nuclear fuel greater than 100 grams would be protected in accordance with §73.51. The 100-gram limit is consistent with the NRC's spent nuclear fuel transportation requirements in §73.37.

[8] *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]

The current requirement for sabotage mitigation of the facility at non-power reactors (i.e., §73.60(f)) would be retained. While spent non-power reactor fuel would not be subject to §73.51, staff concludes that additional protection beyond that described in 10CFR73.60(f) is not required to manage the sabotage risk of spent non-power reactor fuel above that provided to prevent theft or diversion.

Providing additional protection for material that poses a greater sabotage risk fills the regulatory gap discussed in Section 3 and is consistent with the NRC's strategic goal (see Section 9). Moreover, the requirements in Attachment 3 ensure adequate protection against sabotage scenarios associated with malevolent use of plutonium 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. 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, staff proposes to change the existing transportation physical protection requirements based on risk insights and operating experience. As such, **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, staff used the same protective strategies for each SNM Category and material attractiveness level as was developed for fixed sites. 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 requirements 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, **staff proposes six sets of requirements for transportation (i.e., for non-dilute Category I, moderately dilute Category I, highly dilute Category I, non-dilute Category II, moderately dilute Category II, 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 or to protect all their material, non-dilute and dilute, at the higher non-dilute 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 as non-dilute.

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, both of which considered the evolving threat. In particular, the rulemaking considers and addresses, as appropriate, the gaps identified in the Sandia National Laboratory transportation security comparability study reports (SNL, 2013a; SNL, 2013b; SNL, 2013e; SNL, 2013f; SNL, 2013g, SNL, 2013h; SNL, 2013i). Based on risk insights and operating experience discussed in Section 3, staff is proposing several new or modified requirements. These include:

1. **Staff proposes to require licenses or their agents provide for continuous determination of the position of the shipment and communication of the positioning information to the movement control center.** 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.

2. **Staff proposes to require development of specific graduated protective measures and actions to be taken to increase licensee preparedness against a heightened security threat, and 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.** Coordination will leverage existing US Government resources to inform licensees of potential risk associated with proposed shipments.

3. **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 will provide tracking the transportation, periodically communicate with the transporter, and if required, coordinate response forces.

The proposed changes solve the regulatory problems discussed in Section 3 and are consistent with the NRC's strategic goal (see Section 9). Moreover, the new requirements in Attachments 9 - 15 ensure adequate protection against theft or diversion and sabotage scenarios associated with malevolent use of SNM during transport. The table 4-4 summarizes the proposed transportation physical protection requirements.

Table 4-4: Summary Transportation Security Requirements

	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 and diversion and radiological sabotage – Prevent the removal of SNM and other unauthorized activities involving	– 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	– Immediately detect attempts to remove of SNM and notify LLEA to allow recovery of SNM	– Detect attempts to remove of SNM and notify LEA to allow timely recovery of SNM

	SNM – Insider Mitigation Program	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 – Part 26 – including Subpart I	– 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 2000 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	– Controlled access for SNM loading	– Controlled access for SNM loading	– Controlled access for SNM loading

	and transfer areas, transportation security systems, transportation conveyances, escort vehicles, and SNM containers. – Controlled badge program – Control of keys, locks, and other access control devices – Access authorization program per Part 11	and transfer areas, transportation security systems, transportation conveyances, escort vehicles, and SNM containers. – Controlled badge program – Control of keys, locks, and other access control devices – Access authorization program per §73.57, §73.59, §73.61	and transfer areas, transportation conveyances, and SNM containers. – Controlled badge program – Control of keys, locks, and other access control devices – Personnel trustworthiness program	and transfer areas, transportation conveyances, and SNM containers – Controlled badge program – Control of keys, 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	– LLEA Liaison – 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	– Container receipt upon entry into the U.S. – Protection of	– Container receipt upon entry into the U.S. – Protection of	– Container receipt upon entry into the U.S. – Protection of

	shipments while in the U.S.	shipments while in the U.S.	shipments while in the U.S	shipments while in the U.S
Security Program Review	– Annually – Management Review – CAP or event log – Performance evaluation program	– Annually – Management Review – CAP or event log	– Bi-annually – Management Review – CAP or event log	– Bi-annually – Management Review – CAP or event log
Maintenance & Testing	– Required	– Required	– Required	– None
Compensatory Measures	– In TSP	– In TSP	– In TSP	– In TSP
Suspension of Security Measures	– Allowed	– Allowed	– Allowed	– Allowed
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, fitness for duty, and the safety-security 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 3.2, 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. Subsequently, the Commission did not impose by order access authorization 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 similar requirements for nuclear power reactors and non-power reactors in §73.57. Moreover, the existing access-authorization requirements are proposed to remain in place for non-power reactors. To resolve the regulatory gap with respect to access authorization, **staff proposes to add Category I - moderately dilute, Category I - highly dilute, non-dilute Category II, and Category II - moderately dilute licensees to the list of applicable licensees in §73.57; §73.59; and §73.61**.

A robust access-authorization program can manage the risk of insiders aiding or accomplishing misuse of SNM for malevolent purposes. Adding non-dilute Category II and moderately dilute Category II SNM facilities to the list of licensees required to comply with §73.57, §73.59, and §73.61 efficiently and effectively meets legislative mandates and Commission policy. After a final rule is issued, the agency's long-term objective is to rescind these security orders.

Threshold Dose Limit

As discussed in Section 3.4, 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, 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. External dose-rates in the range of several thousand rad per hour would be considered "self-protecting." This dose-rate would be produced by spent nuclear

fuel (i.e., from power reactors, which would be protected in accordance with §73.51) and could be produced by some non-power reactor irradiated fuels. However, the radiation levels for irradiated non-power reactor fuel would decline relatively quickly in days or months. Changing physical protection over these short and potentially variable timeframes is not considered prudent. Staff considers that non-power reactor fuel can be adequately protected considering material attractiveness and dilution as discussed above without relying on external dose-rate as a security feature. However, if licensees wish to consider external radiation dose-rate as a security feature, they would be able to do so under new requirements discussed above that would allow licensees to propose alternative security measures.

Eliminating the use of the external radiation dose-rate threshold will help ensure that SNM is adequately protected in ways consistent with the risk posed by the material.

Fitness for Duty

As discussed in Section 3, staff concluded that there is a regulatory gap and policy inconsistency with respect to managing fatigue for security officers at Category I facilities. Therefore, staff proposes to require Category I licensees to comply with Part 26, Subpart I for security officers. These licensees would be required to ensure against worker fatigue adversely affecting public health and safety and the common defense and security by establishing clear and enforceable requirements for the management of security force worker fatigue that would:

- Establish an approach for fatigue management that takes into account industry practices.
- Provide high assurance that security officers continue to meet their responsibilities for maintaining the common defense/security and ensuring that this critical group is not unnecessarily subjected to fatigue that could reduce alertness or ability to perform duties, sustain attention, analyze problems, make rapid and accurate decisions, communicate information and identify and respond to threats with authority to apply deadly force.
- Prevent consequences that might result from theft or diversion of SNM by an adversary for use in an IND.
- Address the NRC's inconsistent approach of applying fatigue management requirements of Part 26 to some but not all of the security officers that perform equivalent duties (i.e., security officers at nuclear power reactors versus those at Category I facilities).

Effective management of worker fatigue is needed because individuals experience fatigue for many reasons (e.g., long work hours, long commutes, inadequate rest, stressful work, shiftwork, home-life demands, sleep disorders, and workers' varying tolerance to these conditions). Research and literature demonstrate the substantial effects of fatigue (decreased alertness) on an individual to safely/competently perform their duties:

- Lack of adequate days off and extension of workdays or overtime can result in cumulative sleep debt and performance impairment.
- Studies on extended work hours suggest that fatigue-induced personnel impairment can increase human error by a factor of 2 to 3 times.

- Fatigue can impair both physical and mental functions such as alertness, processing complex information, mental and motor responses, performing multiple tasks, and recalling material from memory.

- Deterioration in performance occurs after 12 hours, particularly when combined with work weeks longer than 40 hours.

- An example: The National Transportation Safety Board (NTSB) found that flight crews who had been awake for longer than 12 hours and were involved in accidents made more tactical decision errors than crews who had been awake for a shorter time.

To address fatigue for security officers at Category I facilities, **the staff proposes to apply the current fatigue-management requirements in Part 26, Subpart I to individuals who perform security duties (i.e., personnel performing security duties as an armed security officer, alarm station operator, response team personnel, or watchman) at Category I SNM fixed sites and in transit**. Licensees of these facilities would be required to implement a fatigue-management program to help provide high assurance that security officers will not be impaired from fatigue, can execute their duties according to the site's security plan, and meet regulatory obligations. In pursuing fatigue-management requirements for certain fuel cycle facility licensees, staff does not rule out the possibility that fatigue-management requirements would be considered in the future for other material licensees or other personnel through the direction provided by the Commission in SRM-COMSECY-04-0037 (NRC, 2004c).

Managing the fatigue of security officers at Category I facilities would provide high assurance that they are able to perform their duties safely and competently to deter and prevent theft or diversion of SNM or other malicious events. Therefore, staff believes that regulatory action is warranted to require Category I facility licensees to manage the schedules and work hours of their security force to manage fatigue and to substantially enhance security at these facilities.

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 determined 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, staff is aware of instances in which licensee changes in one discipline presented significant potential challenges to another. For that reason, 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 requirements 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 in one when changes occur in the other.

In keeping with the principles of good regulation, any new requirement should minimize the burden on licensees and should allow licensees to make minor changes without NRC approval. As such, the requirements should not explicitly require communication to the NRC about the implementation and timing of facility changes beyond those already required elsewhere. The new requirements 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 requirement 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.

Staff proposes to modify the requirements in §70.72(a) and 50.59(c) to put in place safety/safeguards interface requirements. The requirements 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 requirements 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. Staff recognizes that implementation of these new requirements would rely to the extent possible on existing programs that manage facility changes and configuration. Incorporation of these new requirements 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 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 staff considered as alternatives to resolve the regulatory problems presented in Section 3. This section explains why the NRC or the licensees cannot take actions to resolve the problems effectively within the existing regulatory framework. The alternatives considered are described and reasons why they were not pursued are discussed.

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

5.1 No Action

Under this alternative, the NRC 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 staff to issue new security orders to new facilities and issue site-specific licensee conditions to address facility- and SNM-specific risk concerns raised in Section 3. This alternative has the greatest regulatory uncertainty for new licensees because they would need to design their physical protection systems based on the regulations also be 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 and 4. This alternative also would not meet the intent of the SRMs discussed in Section 1. Based on the changes in threat environment and risk insights discussed above, the NRC staff does not recommend this 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, these would not be suitable for the large and complex issues described in Section 3. In addition, these two NRC communication tools are for existing licensees. While they could be used to raise the awareness of issues discussed in Section 3, these generic communications cannot impose new requirements or relax existing requirements

on licensees. Therefore, this alternative would not be fully responsive to the intent of the SRMs discussed in Section 1.

5.3 Revise existing regulatory guidance documents

Under this alternative, 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.

Regulatory Guides provide guidance to licensees and applicants on carrying out specific parts of the NRC's regulations, techniques used by the NRC staff in evaluating specific problems 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 and Category II and III facilities in the 1970s and early 1980's. As such and as discussed in Section 10, 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 should not 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.

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. Staff did not pursue this alternative because such documents describe methods that the NRC staff considers acceptable for use in carrying out specific parts of the agency's existing regulations. As discussed above, because regulatory guides 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.

5.5 Issue Site-Specific License Conditions

Under this alternative, NRC 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, 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. Imposing license conditions also affords licensees the opportunity to object, which could result in protracted legal proceedings and decrease the emphasis on adequate protection of SNM. Staff did not pursue this alternative because it is also not directly responsive to the SRMs discussed in Section 1.

Given the limited number of licensees that would be affected by the proposed fitness-for-duty requirements, working with Category I licensees to include Part 26, Subpart I as a license condition or security-plan commitment might be a viable option to rulemaking to address the issues discussed in Section 3. Under this alternative, using NRC resources to undertake this rulemaking effort would be avoided, but the public would be precluded from involvement in such a regulatory action. This alternative would be contingent on licensees' willingness to make such

commitments and the burden to licensees would be the same as with rulemaking. In addition, this alternative would not provide regulatory predictability to new licensees.

5.6 Issue Security Orders to Category I Facilities Regarding Fatigue Controls for Officers

Under this alternative, the NRC would issue security orders to the two Category I facilities for these sites to implement the fatigue management requirements found in 10 CFR Part 26 for security officers only. In conducting the evaluations to develop this regulatory basis, the staff did not identify an immediate public health and safety concern, therefore, an order is not appropriate. Further, the rulemaking process has certain advantages over issuing security orders, namely it allows the public to better participate in the process.

6. Backfit Rule Applicability

As discussed in Section 1, the regulatory basis includes three rulemaking efforts. First, the rulemaking will update physical protection requirements for special nuclear material at fixed sites (*i.e.*, fuel cycle facilities, production and non-power reactor utilization facilities) licensed under 10 CFR Part 50 – to:

- make security requirements imposed by security orders 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 10 CFR Part 50
- improve consistency and clarity of physical security protection requirements at fixed fuel cycle facilities
- consider risk-insights from new National Laboratory studies, operational oversight and inspection activities, 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

Second, the rulemaking will update requirements governing the transportation of special nuclear material consistent with the new security requirements for special nuclear material at fixed sites, as described above. Finally, the rulemaking would apply the NRC fatigue management requirements to security officers for Category I material at fixed sites and during transport.

Entities who are not provided with backfitting protection

This rulemaking will affect production and non-power reactor utilization facilities licensed under 10 CFR Part 50, all fuel cycle facilities licensed under 10 CFR Part 70, and gaseous diffusion plants who seek or hold a certificate of compliance (CoC) from the NRC under 10 CFR Part 76. Of these entities, only fuel cycle facilities licensed under 10 CFR Part 70, and gaseous diffusion plants who seek or hold a CoC from the NRC under 10 CFR Part 76, are accorded backfitting protection.

Part 50 facilities

Production facilities and non-power reactor utilization facilities licensed under 10 CFR 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 10 CFR 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 fuel cycle facilities[9]

Fuel cycle facilities licensed under Part 70 and gaseous diffusion plants who have obtained certificates of compliance under Part 76[10] 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, 10 CFR 70.76 and 10 CFR 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 common defense and security. Hence, the NRC would likely be unable to justify the adoption of

---

[9] 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.

[10] 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.

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 NRC 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 NRC 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. This section summarizes stakeholder interest and views.

During the development of this Regulatory Basis, staff interacted with stakeholders and interested members of the public, other Federal agencies, as well as representatives of foreign governments, to obtain supporting information, views and opinions on the Regulatory Basis. Affected stakeholders for this effort include the NRC-licensed fuel cycle facilities and non-power reactors, other NRC licensees that possess SNM, other Federal agencies and the public. Stakeholder interactions are captured in Table 7-1. The outcomes of these interactions are discussed further below. To increase stakeholder involvement and awareness outside traditional meetings held with domestic and international stakeholders to solicit feedback, the NRC used the following additional channels to obtain stakeholder feedback:

1. The NRC solicited feedback through a Web page dedicated to explaining to the public the material attractiveness and fatigue rulemaking effort associated with 10 CFR Parts 26 and 73 since 2011 (see http://www.nrc.gov/security/domestic/phys-protect/reg-initiatives/10cfr73.html).

2. The NRC held a series of Webinars in the February through May 2014 timeframe to obtain stakeholder feedback on material attractiveness and fatigue rulemaking efforts.

3. The NRC issued the regulatory basis for public comment in a Federal Register Notice in May 2014.

4. The NRC held a public meeting on the regulatory basis to obtain public comments in June 2014.

External Meetings on Material Attractiveness

Staff conducted extensive outreach with other Federal agencies, the domestic industry, and non-governmental organizations about its intent to consider material attractiveness when grading and developing physical protection requirements. The discussion with foreign governments focused primarily on whether staff's approach on considering material attractiveness, when defining 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 being conducted by Los Alamos National Laboratory (LANL), would meet the intent of INFCIRC/225, Revision 5 (IAEA, 2011). However, to avoid misconceptions or confusion, it was also suggested that the NRC should keep its existing table from INFCIRC/225, Revision 5 (IAEA, 2011) and discuss different security measures, adjusted for attractiveness, in the text of regulations.
In addition to the more formal discussions with certain foreign governments, staff took advantage of international meetings to have discussions with six other international partners. The feedback from most of these governments was that the proposed staff approach to material categorization is consistent with INFCIRC/225, Revision 5 (IAEA, 2011).

In addition to the more formal discussions with stakeholders at NRC-sponsored meetings, staff took advantage of meetings sponsored by the Institute of Nuclear Materials Management. Discussions with the domestic industry, including with the U.S. fuel cycle licensees and the

Nuclear Energy Institute (NEI), focused on gaining an understanding of the potential impacts on the industry from any changes to the categorization table when considering material attractiveness and the corresponding physical protection requirements. Feedback from the Category I facilities indicated that staff's approach might allow licensees to relocate some of their operations outside the material access area (MAA). This would reduce the number of workers requiring access to the MAA, resulting in some cost savings to these licensees. Some of the activities that could be relocated include analytical laboratories and engineering/test processes. A fuel cycle facility industry working group put together by the NEI concluded that an approach including attractiveness could make the transport of mixed-oxide fuel more affordable. To document this opinion, NEI sent (Killar, 2009) a letter to the NRC in 2009, supporting a change in the NRC's categorization table to take into account SNM attractiveness.

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. A number of non-governmental organizations have presented papers in publications and at technical conferences that have expressed this concern Representatives from the non-governmental organizations (NGOs) expressed a concern that any changes in physical protection were, in fact, a reduction in security. The original table (Table 4-1) considered by the NRC was seen by some NGOs and echoed by some foreign government representatives as a major reduction in the protection requirements rather than an adjustment that provides more appropriate protection requirements based on the different form of the material. To avoid any confusion, staff made changes to its approach to keep the existing table from INFCIRC/225, Revision 5 (IAEA, 2011) and discuss different security measures, adjusted for attractiveness, in the text of regulations.

NRC Workshops

On February 6, 2014, the NRC hosted a public workshop at NRC headquarters to: (1) explain what a regulatory basis is; (2) explain the objectives of this rulemaking; (3) discuss the timelines associated with stakeholder outreach and completion of major milestones associated with this effort; and (4) discuss material attractiveness. One general comment was that the comment period on the regulatory basis document should allow as much time as possible for stakeholders to comment on this complex issue. In response to inquiries about the supporting LANL studies on material attractiveness, NRC staff explained that the study considers the different forms of SNM at NRC-licensed sites, considers the security requirements at these sites, and considers how credible it would be for an adversary to acquire the SNM through different attack modes.

The next public workshop was conducted on February 20, 2014, at NRC headquarters to discuss: (1) access authorization; (2) safety/safeguards interface; and (3) fixed site physical security. The workshop began with staff referencing the timelines and due dates for the Regulatory Basis and opportunities for stakeholder input and feedback. Specifically, staff requested that licensees provide input and feedback associated with cost and impacts to licensees for changes proposed in the Regulatory Basis (once the proposal is issued for public comment). Discussions included comments that the proposed access authorization approach might result in the possible expansion of the access-authorization requirements and whether the NRC intends to rescind any security orders related to access authorization. A concern was expressed that the proposed new safety/safeguards requirement may lead to additional documentation requirements. During stakeholder discussions it was explained that the regulations and regulatory guides will provide clarity on which categories different forms of SNM would be placed. In response to other comments, staff stated that it does not anticipate any

changes to the physical protection measures for Category III licensees based on the current regulations and security orders. However, some Category I licensees might see some changes to the requirements for physical protection requirements under this proposal. As for Category II licensees, staff stated that those licensees could see significant changes because security orders were not issued given the limited number of potential licensees. During discussions regarding implementation (i.e. maintaining the highest security level vs. different security zones), staff stated the desire was to maintain a performance-based approach where the licensee could develop an implementation strategy that determines the best approach. In response to concerns expressed over the proposal to use a corrective action program, staff stated that it would revise the proposal to allow a choice on whether to capture the security-related issues in a corrective action program or a security event log. Due to a concern about the proposed protection levels for Category I dilute materials, staff stated that it is still working on the appropriate protection measures and noted that Category I dilute materials are in a bulkier form, more difficult to acquire, and more difficult to process for use in an IND.

The third workshop on April 9, 2014, focused on sabotage and transportation security. Discussions focused on if the NRC is synchronizing its efforts with the U.S. Department of Transportation (DOT). In response to comments, the staff noted that it is synchronizing its efforts with DOT and other federal agencies. Stakeholders questioned if there would be any changes (physical protection measures) associated with the transport of UF_6 cylinders for Category III licensees in this effort. The staff responded that it does not anticipate any significant changes.

Fatigue

With respect to the fatigue-management effort for security officers at certain facilities, staff conducted outreach with both fuel cycle facilities and NEI on multiple occasions directly or at conferences. Staff explained that its basis is broad and includes: (1) considering the potential consequences at Category I facilities when officers are fatigued and fail to execute their duties; (2) the inconsistent approach the NRC applies to fatigue management regulations, given that officers at power reactor facilities and at Category I facilities perform the same duties in that they must defend against the DBT; and (3) limited information that indicates that some facilities have not managed officer work hours at their sites and might have subjected their officers to acute/cumulative fatigue, all of which could lead to degradation in officer performance. After completion of the survey to determine officer work hours at seven fuel cycle facilities, staff shared its results and initial assessment with NEI and stakeholders. Additionally, staff has explained its intention that officers at Category I facilities would fall under the same fatigue-management requirements of Part 26 as security officers and other select groups at nuclear power reactors. In meetings with industry, and in its April 2013 letters submitted to the NRC (Schlueter, 2013; Pietrangelo, 2013), industry disagreed with the consideration of fatigue management requirements at this time because they believe there is no trending information and no enforcement actions or information that would form the regulatory basis for such a rule.

Table 7-1: Outreach Initiatives for the Regulatory Basis

Date	Out Reach Item	Description
05/13/2010	Meeting between the Nuclear Energy Institute (NEI) and the Nuclear Regulatory Commission (NRC) to discuss the Reprocessing Regulatory Framework	Discussed the 10 CFR Part 73 rulemaking effort.

09/09/2010	Reprocessing Public Workshop in Rockville, MD	Discussed the 10 CFR Part 73 rulemaking effort.
10/19/2010	Reprocessing Public Workshop in Albuquerque, NM	Discussed the 10 CFR Part 73 rulemaking effort.
03/24/2011	Launch NRC Web Page	Allowed the public to follow the 10 CFR Parts 26/73 rulemaking effort.
05/24/2011	Briefing for representatives of the U.S. Department of Energy (DOE)/National Nuclear Security Administration's (NNSA's) Office of Defense Nuclear Security, Office of Nuclear Safeguards and Security, and Office of Health, Safety and Security, as well as the U.S. Department of State	Discussed the 10 CFR Part 73 rulemaking effort.
05/25/2011	Briefing for representatives of the Australian Safeguards and Non-Proliferation Office	Discussed the 10 CFR Part 73 rulemaking effort.
06/06/2011	Public meeting on the Fuel Cycle Oversight Process in Rockville, MD	Discussed the 10 CFR Part 73 rulemaking effort.
06/07/2011	Briefing for representatives of the Spanish Nuclear Safety Council	Discussed the 10 CFR Part 73 rulemaking effort.
06/08/2011	Fuel Cycle Information Exchange (FCIX) public meeting in Rockville, MD	Discussed the 10 CFR Part 73 rulemaking effort.
06/22/2011	Reprocessing Public Workshop in Augusta, GA	Discussed the 10 CFR Part 73 rulemaking effort.
07/13/2011	Briefing of representatives of NNSA's Office of Secure Transportation (OST)	Discussed the 10 CFR Part 73 rulemaking effort.
07/21/2011	Briefing for representatives of the Australian Safeguards and Non-Proliferation Office and the UK Office of Civil Nuclear Security (OCNS)	Discussed the 10 CFR Part 73 rulemaking effort.
8/25-26/2011	Briefing for the Canadian Nuclear Safety Commission in Ottawa, Canada	Discussed the 10 CFR Part 73 rulemaking effort.
09/06/2011	Briefing for Spanish representatives in Madrid, Spain	Discussed the 10 CFR Part 73 rulemaking effort.
09/09/2011	Briefing for UK OCNS and Ministry of Defence (MoD) representatives in Oxford, UK	Discussed the 10 CFR Part 73 rulemaking effort.
11/09/2011	Briefing for French representatives in Paris and Fontenay Aux Roses, France	Discussed the 10 CFR Part 73 rulemaking effort.
11/11/2011	Briefing for UK OCNS and MoD representatives in London and Oxford, UK	Discussed the 10 CFR Part 73 rulemaking effort.
04/26/2012	Briefing for the Argentina Nuclear Regulatory Authority in Buenos Aires, Argentina	Discussed the 10 CFR Part 73 rulemaking effort.
06/14/2012	FCIX public meeting in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
08/01/2012	Updated NRC Web page	Allowed the public to follow the 10 CFR Parts 26/73 rulemaking effort.
09/13/2012	Conference call with NEI and Fuel Cycle Facilities	Discussed survey results of officer work hours at seven fuel cycle facilities and the 10 CFR

		Part 26 rulemaking effort.
12/01/2012	Security Regulators Conference in Rockville, MD	Discussed the 10 CFR Part 73 rulemaking effort.
12/3-5/2012	Discussions with representatives of France, UK, and Russia at International Security Regulators Conference	Discussed the 10 CFR Part 73 rulemaking effort.
1/15-16/2013	Presentations to le ministère de l'Écologie, du Développement durable et de l'Énergie (MEDDE), Secrétariat général de la défense et de la sécurité nationale (SGDSN), and Commissariat à l'énergie atomique et aux énergies alternatives (CEA) of the government of France.	Discussed the 10 CFR Part 73 rulemaking effort.
01/17/2013	Presentation to the Department of Energy & Climate Change, MoD, Office for Nuclear Regulation (ONR), and Cabinet Office of the UK.	Discussed the 10 CFR Part 73 rulemaking effort.
04/02/2013	Presentation at Institute of Nuclear Materials Management's (INMM's) Reducing Risk Workshop in Washington, DC	Discussed the 10 CFR Part 73 rulemaking effort.
4/8-12/13	Discussion with representatives of UK, Netherlands, Japan, and Russia at NUSAT CM in Vienna, Austria	Discussed the 10 CFR Part 73 rulemaking effort.
04/10/2013	Presentation to the NEI Fuel Cycle Meeting in Atlanta, GA	Discussed the 10 CFR Parts 26/73 rulemaking effort and cyber and chemical security.
6/4-6/13	Meetings with MEDDE and SGDSN of the government of France in Albuquerque, NM	Discussed the 10 CFR Part 73 rulemaking effort.
06/10/2013	Cumulative Effects of Regulation Meeting in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
06/13/2013	FCIX in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
7/1-5/13	Presentation at the International Atomic Energy Agency (IAEA) Security Conference in Vienna	Discussed the 10 CFR Part 73 rulemaking effort.
7/15-18/13	Presentations at the INMM Annual Meeting in Palm Desert, CA	Discussed the 10 CFR Part 73 rulemaking effort.
07/23/2013	Meetings with CEA, SGDSN of the government of France and the MoD, ONR, and Cabinet Office of the UK in Washington, DC	Discussed the 10 CFR Part 73 rulemaking effort.
07/24/2013	Updated NRC Web page	Allowed the public to follow the 10 CFR Parts 26/73 rulemaking effort.
09/19/2013	Presentation at Ohio State University Nuclear Forum, Columbus, OH	Discussed the 10 CFR Part 73 rulemaking effort.
09/24/2013	The National Organization of Test, Research and Training Reactors – Annual Meeting	Discussed the 10 CFR Part 73 rulemaking effort
10/01/2013	Cumulative effect of regulation Meeting in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
12/16/2013	Discussion with representatives of the Japan Nuclear Energy Safety Organization (JNES) and Japanese Nuclear Regulation Authority (JNRA) in Rockville, MD	Discussed the 10 CFR Part 73 rulemaking effort.
01/14/2014	Cumulative effect of regulation Meeting in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.

01/27-28/2014	Discussions with representatives of France and UK	Discussed the 10 CFR Part 73 rulemaking effort.
1/30-31/2014	Discussions with representatives of France and UK	Discussed the 10 CFR Part 73 rulemaking effort.
1/30/2014	Updated NRC Web page	Allowed the public to follow the 10 CFR Parts 26/73 rulemaking effort.
02/06/2014	Public Meeting and Webinar in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
2/11-12/2014	Panel Discussion at INMM Workshop on Risk-Informing Security, Stone Mountain, GA	Discussed the 10 CFR Part 73 rulemaking effort.
2/18/2014	Updated NRC Web page	Allowed the public to follow the 10 CFR Parts 26/73 rulemaking effort.
02/18/2014	The National Organization of Test, Research and Training Reactors – Executive Committee Meeting	Discussed the 10 CFR Part 73 rulemaking effort
02/20/2014	Public Meeting and Webinar in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
03/05/2014	Cumulative effect of regulation Meeting in Rockville, MD	Discussed the 10 CFR Parts 26/73 rulemaking effort.
03/13/2014	INMM Meeting at George Washington University, Washington, DC	Discussed the 10 CFR Part 73 rulemaking effort.
03/18/2014	Discussions with French representatives of the World Institute for Nuclear Security (WINS), a non-government agency	Discussed the 10 CFR Part 73 rulemaking effort.
03/19/2014	Discussions with representatives of India's Bhabha Atomic Research Centre	Discussed the 10 CFR Part 73 rulemaking effort.
4/9/2014	Public Meeting and Webinar in Rockville, MD	Discussed the 10 CFR Part 73 rulemaking effort.

8. Cost/Impact Considerations

This section discusses cost and other impacts for the requested changes presented in Section 4. 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 based on staff's assessment and input from stakeholders. A more detailed cost/impact evaluation would 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 or applicants for such license under 10 CFR Part 70 and non-power reactors.

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 10 CFR Part 70 and non-power reactors.

Safety/Safeguards Interface - The inclusion of a safety/safeguards interface requirement would be intended for all current fuel cycle licensees or applicants for such license under Part 70 and non-power reactors These provisions would not be applicable to Part 70 licensees not subject to §70,72.

Fitness-for-Duty Impacts - The inclusion of fatigue management requirements (e.g., work-hour controls) in accordance with Part 26, Subpart I would apply to security officers at Category I facilities.

8.2 Potential Licensee Impacts

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. It is expected that, for most existing licensees, the physical protection program activities currently undertaken would not significantly change and, therefore, the impact on most licensees will be small. Given the improvements provided by considering material attractiveness, it is possible that some facilities might choose to modify their current physical protection programs to take advantage of changes in physical protection requirements for material that is less attractive. This would be especially true for non-power reactors. In these cases, licensees would be impacted in making changes to security plans, implementing procedures, and physical protection equipment and barriers, but the overall burden would be reduced.

Although the physical protection program activities are expected to be essentially the same as current activities, existing licensees would need to modify security plans and implementing procedures to match the new requirements. However, the new requirements 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 requirements was revised to add clarity that should reduce regulatory uncertainty and ultimately reduce the burden on licensees.

As with any new requirement, licensees would need to raise awareness of these new requirements. The impact of potential additional training requirements would likely occur early on because most of the effort would be in the development of the knowledge and applicability of the new requirements. 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.

Transportation Physical Protection - The NRC recognizes that individuals transporting SNM have physical protection programs that address the existing regulations. It is expected that, for most parties, arranging the transportation physical protection program activities currently undertaken would not significantly change; and therefore, the impact on most licensees will be small. Given the improvements provided by considering material attractiveness, it is possible that some parties might choose to modify their current transportation physical protection programs to take advantage of changes in physical protection for material that is less attractive. In these cases, licensees would be impacted in making changes to security plans, implementing procedures, and physical protection equipment, but the overall burden would be reduced. Although the transportation physical protection program activities are expected to be essentially the same as those currently performed, modification of the existing security plans and implementing procedures would be required to match the new requirements. However, the new requirements are intended to be more performance-based and less prescriptive; therefore, licensees would be provided flexibility in tailoring the overall transportation physical protection program. 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) and

other involved parties. In addition, the structure of the new requirements was revised to add clarity that should reduce regulatory uncertainty and ultimately reduce the burden on licensees.

As with any new requirement, licensees would need to raise awareness of the new requirements. The impact of potential additional training requirements would likely occur early on because most of the effort would be in the development of the knowledge and applicability of the new requirements. 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.

Safety/Safeguards Interface - The NRC recognizes that various facility programs might address the safety/safeguards interface to some extent. Examples might include reviews of process changes, procedure changes, and maintenance order review processes. It is the NRC's view, given the large effort that has been focused on safety of plant processes as required by Part 70, Subpart H in recent years and the requirements of 10 CFR 50.59, that a new safety/safeguards interface requirement will primarily result in an expectation that safeguards impacts be fully considered. It is not the intent of a new safety/safeguards interface requirement to impose new broad programmatic requirements on licensees.

As with the current 10 CFR 73.58 interface requirement for reactors, it is expected that licensees would rely on, and take credit for, currently existing processes to the maximum extent practical. If current work-management processes and configuration-control programs are adequately controlling facility activities to prevent adverse interactions between safety/safeguards, these processes should continue to be used. However, in complying with such a new requirement, 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 plant activities in response to the new requirement, the maximal use of existing programs should lessen the associated cost and burden.

As with any new requirement, licensees would need to raise awareness of the safety/safeguards interface. The impact of potential additional training requirements would likely occur early on because most of the effort would be in the development of the knowledge and applicability of the new requirement. 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.

Fitness for Duty Impacts - The NRC recognizes that the current Category I facilities have either a policy in place or a practice to address some fatigue aspects for security officers at their sites. While the Category I facilities have some provisions in place to address security officer fatigue, it is expected that these two sites, in complying with the fatigue management requirements in Part 26, will incur additional costs. Additionally, sites may need to hire additional security officers at the site to meet the work-hour controls in Part 26, which would increase licensee burden. Nuclear power reactors have taken advantage of computer software that allows them to efficiently track security officers work hours in order to meet regulatory requirements in Part 26.

The new requirement will give the licensee the flexibility to grant a waiver of the work-hour controls in Part 26 if it is determined that:

1. The waiver is necessary to maintain site security; and
2. The supervisor assesses the individual and determines that there is reasonable assurance that the individual will be able to safely and competently perform their duties during the additional work period for which the waiver will be granted.

As with any new requirement, licensees would need to raise awareness of these new work-hour controls for security officers. This might lead to additional costs associated with training security officers and updating or developing new procedures to implement these new regulatory requirements. As noted above, it is expected that at least one of the two licensees will make optimal use of existing programs in place, which should reduce the cost and burden by using and updating existing procedures and training programs.

8.3 Impact on the NRC

Fixed-Site Physical Protection - The new fixed-site physical protection requirements would require inspection resources from the regional NRC staffs to support follow-on inspections of licensee programs. Also, as discussed in Section 10, supporting guidance would have to be evaluated and revised or developed.

Transportation Physical Protection - The new transportation physical protection requirements would require inspection resources from the regional NRC staffs to support follow-on inspections of licensee programs. Also, as discussed in Section 10, supporting guidance would have to be evaluated and revised or developed.

Safety/Safeguards Interface – A new rule in the area of safety/safeguards interface capabilities would require inspection resources from the regional NRC staffs to support follow-on inspections of licensee programs. Also the need for supporting guidance would have to be evaluated. Because of the expected applicability of existing licensee programs and existing guidance for the similar 10 CFR 73.58 requirement for reactors, additional resource needs should be minimal.

Fitness for Duty Impacts - It is expected that this new rule will require devoting some inspection resources from regional NRC staff to support follow-on inspections of licensees' security officer fatigue/work-hour programs at these two sites. The NRC is expected to take advantage of its established inspection programs associated with fatigue/work-hour controls for security officers at nuclear power reactors so that any new additional resource needed to extend this effort to this class of licensees should be minimal.

8.4 Impact on State, Local, or Tribal Governments

The proposed changes are unlikely to affect State and local government resources. Agreement State authorities would not be required to adopt a similar requirement for their licensees. 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. 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, 2012b). 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 adequate protection of public health and safety and the environment.
- Security: Ensure adequate protection in the secure use and management of radioactive materials.

To achieve the security strategic goal, the NRC developed the following security-goal implementation strategies.

1. Conduct oversight of licensee security performance.
2. Use relevant intelligence information and security assessments to maintain realistic and effective security requirements and mitigation measures.
3. Share security information with appropriate stakeholders and international partners.
4. Control the handling and storage of sensitive security information and the communication of information to licensees and Federal, State, local and Tribal governments.
5. Support Federal response plans that employ an approach to the security of nuclear facilities and radioactive material that integrates the efforts of licensees and Federal, State, local, and Tribal governments.
6. Use risk-informed approaches to inform regulatory controls for security.
7. Maintain the programs for controlling the security of radioactive sources and strategic special nuclear material in ways commensurate with their risk, including taking actions required by the *Energy Policy Act of 2005*.

8. Promote U.S. national security interests and nuclear nonproliferation policy objectives for NRC-licensed imports and exports of byproduct source and special nuclear materials and nuclear equipment.

9. Manage the risk to information and systems to ensure the integrity of cyber security at regulated facilities.

10. Prevent instances of significant unauthorized disclosures of classified or Safeguards Information.

The actions proposed in this Regulatory Basis support the NRC's Strategic Plan in multiple areas.

Implementation strategy 2 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 and security assessments. The proposed SNM physical protection requirements also considered risk insights, operational and oversight activities, 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.

Following the NRC's rulemaking process (which includes sharing of information with stakeholders and international partners) supports implementation strategy 3. The security orders discussed in Section 3.2 required licensees to promptly implement a range of physical protection measures because of the change in the threat environment. These security orders were issued because the NRC could not delay the implementation of new security requirements using its normal rulemaking process because of the length of time it takes to issue a final rule (multiple years) and have licensees implement that rule. The NRC now uses the rulemaking process to conduct its business in a more transparent manner that will enable stakeholders to participate and provide feedback on these security order requirements (when possible). Moreover, as discussed in Section 7, staff has conducted extensive stakeholder interactions including international partners.

Using risk insights discussed in Section 3 to propose changes to the SNM physical protection at fixed sites and during transport supports implementation strategy 6. Many of the risk insights were based on National Laboratory studies and include material attractiveness, consideration of external radiation dose-rate threshold as a security feature, sabotage protection, and security officers' fitness for duty. 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. In addition, the proposed fitness-for-duty requirements for Category I security officers considers risk of SNM being successfully acquired by an adversary as a result of security officers' fatigue and a failure to implement the site's physical protection plan.

Furthermore, the LANL studies will support the NRC's efforts (under implementation strategy 7) 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 to an adversary for use in an IND. The rulemaking puts access-authorization requirements mandated by the Energy Policy Act of 2005 into regulations. The rulemaking efforts will also result in updating and refining the NRC's SNM inspection program as well as regulatory guidance. These actions will improve the effectiveness of security programs.

10. Guidance Documents

The guidance development associated with these rulemaking efforts 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 Cat 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. 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 each 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," and

- RG 5.27/ DG 5038, "Special Nuclear Material Doorway Monitors."

- RG 5.73, "Fatigue Management for Nuclear Power Plant Personnel."

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), 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),

- 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), and

- 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 transportation physical protection. In addition, conforming changes would be needed for IP 81502, “Fitness for Duty Program.” With respect to IMC 2545, approximately 6 inspection procedures would need to be updated for non-power reactor physical protection.

To the extent possible, all the revised and new guidance documents will 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 efforts are being tracked by the Commission. As such, these rulemaking efforts are 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. The following table summarizes the resources in the current budgeting cycle for the three rulemaking efforts.

Effort	Fiscal Year	Staffing (FTE)	Contract ($K)
Enhanced Security at Fuel Cycle Facilities/Part 73	FY 15	3.3	91
	FY 16	3.3	91
Special Nuclear Material Transportation Security	FY 15	0.5	0
	FY 16	0.5	0
Fitness-for-Duty – Security Force Fatigue at Nuclear Facilities/Part 26	FY 15	0.2	0
	FY 16	0.2	0

12. Timing

The rulemaking efforts included in this Regulatory Basis have been assigned a "high priority" and are being tracked by the Commission. The proposed rule and associated guidance are scheduled to be submitted to the Commission on or before May 3, 2016. The final rule is scheduled to be to submitted to the Commission on or before November 13, 2017. 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).

Akerstedt, T. 2003. Shift work and disturbed sleep/wakefulness. *Occupational Medicine* 53(2):89-94.

Åkerstedt, T. 2007. Altered sleep/wake patterns and mental performance. *Physiology and Behavior* 90:209-218.

Banks S, Dinges DF. 2007. Behavioral and physiological consequences of sleep restriction in humans. Journal of Clinical Sleep Medicine 3(5):519-528.

Belenky, GL, Wesensten, NJ, Thorne, D, Thomas, M, Sing, H, Redmond, DP, Russo, MB, and and Balkin, T. 2003. Patterns of performance degradation and restoration during sleep restriction and subsequent recovery: a sleep dose-response study. *Journal of Sleep Research* 12:1-12.

Balkin, T. 2003. Patterns of performance degradation and restoration during sleep restriction and subsequent recovery: a sleep dose-response study. *Journal of Sleep Research* 12:1-12.

Dawson D, Reid K. 1997. Fatigue, alcohol and performance impairment. *Nature* 388:235–237.

Dinges DF. 1995. An overview of sleepiness and accidents. *Journal of Sleep Res*earch 4(2):4-11.

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).

Durmer, J., and D. Dinges. 2005. Neurocognitive consequences of sleep deprivation. Seminars in Neurology 25:117-129.

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).

Harrison, Y., and Horne, JA. 2000. The impact of sleep deprivation on decision making: a review. Journal of Experimental Psychology: Applied 6(3):236-249.

Hockey, G. 1970. Changes in attention allocation in a multi-component task under sleep deprivation. British Journal of Psychology 61:473-480.

Horne, J. 1988. Sleep loss and "divergent" thinking ability. Sleep 11(6):528-536.

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).

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.

Krueger GP. 1989. Sustained work, fatigue, sleep loss and performance: A review of the issues. Work and Stress 3(2):129-141.

Lamond, N, and Dawson, D. 1999. Quantifying the performance impairment associated with fatigue. Journal of Sleep Research 8:255-262.

Lorist, M, Klein, M, Nieuwenhuis, S, De Jong, R, Mulder, G, and Meijman, T. 2000. Mental fatigue and task control: planning and preparation. Psychophysiology 37(5):614-625.

Monk, TH, and Carrier, J. 2003. Shift worker performance. Clinics in Occupational and Environmental Medicine 2:209-229.

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 (2003), “Issuance of Order for Compensatory Measures Related to Fitness-for-Duty Enhancements Applicable to Nuclear Facility Security Force Personnel”, April 29, 2003, ADAMS Accession No. ML ML030980015.

NRC (2004a), “Fitness-for-Duty Orders to Address Fatigue of Nuclear Facility Security Force Personnel,” COMSECY-04-0037, June 21, 2004, ADAMS Accession No. ML040790094.

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

NRC (2004c), “Fitness-for-Duty Orders to Address Fatigue of Nuclear Facility Security Force Personnel,” SRM-COMSECY-04-0037, September 1, 2004, ADAMS Accession No. ML042450533.

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, “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), “Strategic Plan: Fiscal Years 2008–2013,” NUREG-1614, Vol. 5, February 15, 2012, ADAMS Accession No. ML12038A003.

NRC (2012c), “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.

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)

Pilcher, JJ, and Huffcutt, AI. 1996. Effects of sleep deprivation on performance: a mega-analysis. Sleep, 19(4):318-326.

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.

Reyes, Luis A (EDO) (2005) memorandum to NRC Chairman Diaz, NRC Commissioner McGaffigan, NRC Commissioner Merrifield, NRC Commissioner Jaczko, NRC Commissioner Lyons, "Fitness-For-Duty Rulemaking to Address Concerns Regarding Fatigue of Personnel at Material Licensee Facilities," April 29, 2005, ADAMS Accession No. ML050890002 (not publicly available)

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).

Totterdell, P, Spelten, E, Smith, L, Barton, J, and Folkard, S. 1995. Recovery from work shifts: how long does it take? The Journal of Applied Psychology 80(1):43-57.

Van Dongen, HPA, Maislin, G, Mullington, JM, and Dinges, DF. 2003. The cumulative cost of additional wakefulness: dose-response effects on neurobehavioral functions and sleep physiology from chronic sleep restriction and total sleep deprivation. Sleep 26(2):117–126.

Van Dongen, HPA, and Dinges, DF. 2005. Circadian rhythm in sleepiness, alertness and performance. In Kryger MH, Roth T, Dement WC (Eds.). Principles and Practice of Sleep Medicine, 4th Ed. Philadelphia, PA: WB Saunders. Pp. 435–443.

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).

Williamson, A, and Feyer, A. 2000. Moderate sleep deprivation produces impairments in cognitive and motor performance equivalent to legally prescribed levels of alcohol intoxication. Occupational and Environmental Medicine 57:649-655.

Williamson, A, Lombardi, S, Folkard, S, Stutts, J, and Courtney, T. 2011. The link between fatigue and safety. Accident Analysis and Prevention 43:498-515.

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*
FRN	*Federal Register* Notice
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 – Technical Basis for Establishing Security Requirements for Protecting Special Nuclear Materials against Theft or Diversion at NRC-Licensed Facilities or during Transport [Classified]

Attachment 2 – Fitness for Duty

Background

Fatigue is degradation in an individual's cognitive and motor functions resulting from inadequate rest, long periods awake, and sustained and or demanding mental or physical effort. Fatigue causes a progressive reduction in alertness and cognitive abilities and an increase in sleepiness. Worker fatigue is a growing concern across many different industries because it adversely affects the ability of individuals to perform their duties safely and competently such by degrading alertness, attention, memory, decision making, communication, and teamwork. Fatigue in security officers is especially a concern because of the need for security officers to find, assess, and react appropriately to potential threats.

Current U.S. Nuclear Regulatory Commission (NRC) regulations applicable to nuclear power plant licensees define and address:

- Acute fatigue, which results from causes such as restricted sleep, sustained wakefulness, or task demands over occurring within the past 24 hours.

- Cumulative fatigue, which results over consecutive sleep-wake periods resulting from inadequate rest during which a sleep debt builds that requires repayment before the accumulated fatigue is eliminated (Belenky et al., 2003).

- Circadian variations in alertness and performance, which mean the increases and decreases in alertness and cognitive/motor functioning caused by human physiological processes (e.g., body temperature, release of hormones) that vary on an approximately 24-hour cycle.

Individuals experience fatigue for many reasons that include:

- long work hours and long commutes
- inadequate rest
- home-life demands
- stressful, strenuous, or monotonous work conditions
- shift work, especially rotating shifts
- sleep disorders
- working alone, especially on jobs that require vigilance with little physical activity

Lack of adequate days off and extended workdays (such as those extended by working overtime) can result in cumulative sleep debt and performance impairment. In addition, research has shown that environments that offer lower stimulation might bring on fatigue and make it harder for individuals to focus and pay attention, particularly when performing monotonous tasks (Harrison and Horne, 2000). This will result in reducing an individual's ability to react quickly to malicious events and in increasing the likelihood of an individual failing to find key pieces of information that might help with assessing a malicious event and determining the appropriate response. Because of the nature of their work (monotonous tasks and low stimulation environments), security officers often experience conditions that cause fatigue.

In 2003, the NRC obtained information provided voluntarily by certain materials licensees about the work hours of their security officers. This information revealed that some security officers were working large amounts of overtime with the potential for experiencing both acute and

cumulative fatigue. Staff believed that fatigue-related requirements were necessary for the security officers and proposed to the Commission to issue fatigue-management requirements for certain material licensees similar to those required at nuclear power reactors through orders. Staff held ten public meetings to receive comments on these proposed orders from the public and the five different classes of material licensees (i.e., Category I fuel cycle facilities, decommissioned reactors, gaseous diffusion plants, independent spent fuel storage installations (ISFSIs), and uranium conversion facilities). Staff reviewed comments for incorporation into the orders and sent the proposed orders to the Commission for review on June 21, 2004 (NRC, 2004a). On September 1, 2004, the Commission directed the staff to pursue rulemaking instead of orders for those materials facilities (see the list above) for which the staff believes fatigue-related requirements are necessary for the appropriate personnel (NRC, 2004c). On April 29, 2005, staff provided a progress report to the Commission (Reyes, 2005) regarding its rulemaking efforts, indicating that the next steps to address fatigue were to determine the categories of materials licensees, the job duty groups at licensee facilities, and the specific fatigue-management requirements to apply in the proposed rulemaking.

Discussion

In 2011 and 2012, to help determine whether security personnel at fuel cycle facilities were working excessive hours, the NRC requested that fuel cycle facilities licensees voluntarily provide data on the work hours of each security officer at their facility for a two-month period. Seven licensees provided these data: two licensees of Category I facilities and five licensees of Category III facilities. Each responding facility provided work-hour records for all security officers employed during the two-month interval for which the data were provided. The data request did not impose an excessive administrative burden on the licensees because licensees routinely generate and archive these data in order to pay workers for the hours they work. NRC staff reviewed and analyzed the data at both the facility and individual level for each facility (i.e., all security officers that fill a non-administrative or non-management role).

The data provide information useful for this analysis. Nevertheless, it is critical to acknowledge a number of limitations associated with the data. First, although the data provided for each facility covers a two-month period, the actual start and end dates of the two-month period vary from facility to facility. Consequently, the data provided by the licensees cover a different number of weeks, ranging from eight to ten. The nature of the data limits the accuracy of analyses of conformance to "rolling" limits, which must be continuously met during each specified time interval (i.e., any 24-hour, 48-hour, or 7-day interval).[11] Because of the short timeframe of the data, the data set represents a "snapshot" of the security officers' work hours at these facilities and cannot be interpreted as representing typical work-hour patterns at the facilities. Furthermore, it is important to remember that the data do not include information on a number of variables known to affect fatigue, such as shift rotation schedules, days off, and break times. Finally, no data were included on the employment status of the security officers. Records for some individuals show strings of zero work hours and others show fewer than 30 hours for some weeks, but it is not clear whether these anomalies are a result of personnel attrition, new hires, vacations, breaks, or part-time employment status. Without additional information, it is not possible to characterize the work status of each of the employees accurately. Thus, it is invalid to assume that all the security officers employed at the seven facilities were full-time staff during the entire reporting period.

[11] Consequently, the analysis probably underestimates the number of times rolling limits were exceeded.

For these reasons, this analysis focuses on two of the work-hour controls specified in 10 CFR Part 26: 10 CFR 26.205(d)(1)(iii) [12] and 10 CFR 26.205(d)(7).[13] It is important to recognize that the work hours submitted by the licensees did not provide the level of detail sufficient to exclude work hours from the total hours worked as a results of periodic drill, shift turnover, etc. (i.e., exclusions in §26.205(b)). The analysis identifies the frequency with which those work-hour controls would have been exceeded by the security officers at the seven fuel cycle facilities had those facilities been subject to the controls. Analysis was performed at the level of the individual employee as well as the facility level. It is important to emphasize that these facilities had no requirement to meet these work-hour limits.

Table Att 2-1 lists the number of instances in which an individual worked more than 72 hours in one of the calendar weeks included in the data set. Note that because the start and end dates of the reporting period vary for each licensee, the time unit markers (W1, W2…W10) in all the tables in this section serve as a counting mechanism only, and do not state that the observations for that time unit occurred during the same calendar week. In addition, note that these data are total hours worked during a calendar week and therefore do not provide an accurate indication of how often the 72-hours in 7-days limit would have been exceeded, if assessed on a rolling basis.

As seen in Figure Att 2-1, in five out of the nine weeks for which data were provided, one worker at Facility I (Category I) exceeded 72 hours of work per week; three of these were in consecutive weeks. At Facility V (Category I), there were sixty-eight (68) instances of a worker exceeding 72 hours per week over the 9-week period, with at least one worker exceeding this limit in eight (8) consecutive weeks. During one particular week (W3), twenty-three (23) workers exceeded this limit. Notably, at Facility V, at least one individual worked eighty-eight (88) hours in one week, which is 16 hours over the 72-hour limit set forth in 10 CFR 26.205(d)(3)(iii). Among the Category III facilities, with the exception of Facilities II and III, none of the workers exceeded the 72-hour-per-week limit during the periods reported. Facility II had one (1) worker above the limit in two non-consecutive weeks. At Facility III there were twenty-six (26) instances of workers exceeding the limit, with one or more workers above the limit every week during the 10-week reporting period.

The number of workers logging long work weeks at both Category I licensees and at two of the Category III licensees indicates that it is not unusual for security officers at these facilities to be working more hours per week than would be allowed if the facilities were subject to the work-hour controls of Part 26. It is noteworthy that the greatest numbers of workers exceeding 72 hours per week occurred at Facility V, a Category I facility. Workers at the two Category I facilities also had the highest reported hours per week, with the maximum work week at Facility V during this relatively short reporting period reaching 88 hours.

---

[12] An individual's work hours may not exceed 72 work hours in any 7-day period.

[13] Individuals may not work more than a weekly average of 54 hours, calculated using an averaging period of up to six weeks, which advances by seven consecutive calendar days at the end of every averaging period.

Table Att 2-1. Counts of Workers Who Worked More Than 72 Hours in a Calendar Week

Category	Facility ID	Reporting Period	# of Weeks	Max Hours per Work Week	# of Workers Exceeding 72 Hours per Week										
					W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	Total
I	I	7/4/2011 to 9/4/2011	9	75.8	1	1	1	0	0	1	0	0	1	N/A	5
	V	9/1/2011 to 10/31/2011	9	88	14	4	23	7	9	1	7	3	0	N/A	68
III	II	12/26/2011 to 3/4/2012	10	76	0	0	1	0	1	0	0	0	0	0	2
	III	8/26/2011 to 11/3/2011	10	75.25	1	1	1	4	1	5	4	1	5	3	26
	IV	9/11/2011 to 11/19/2011	10	59.5	0	0	0	0	0	0	0	0	0	0	0
	VI	10/3/2011 to 11/27/2011	8	67.5	0	0	0	0	0	0	0	0	N/A	N/A	0
	VII	9/10/2011 to 11/18/2011	10	60.5	0	0	0	0	0	0	0	0	0	0	0

To estimate the number of instances in which workers at these facilities exceed the maximum average work-hour (MAWH) limit of 54 hours delineated in 10 CFR 26.205(7), the NRC staff calculated the 6-week rolling averages for each worker for all the weeks included in each licensee's reporting period. Because of differences in the number of 7-day weeks in the reporting periods of the licensees, the number of rolling averages for each facility is non-uniform, ranging from 3 to 5. Because the last week of the 2-month period for Facility V was not a full week, the data for that week were excluded from the calculation of the rolling average. This left Facility V with only three complete 6-week intervals over which the rolling average could be calculated. Table Att 2-2 shows the incidence of workers who exceeded the MAWH limit of 54 hours per week averaged over each 6-week interval. It also shows the maximum average hours per week reported at each facility during a 6-week period. In at least one of the 6-week rolling periods included in the 2-month reporting period, both of the Category I facilities and one of the Category III facilities had workers whose weekly average was over 62 hours per week. At Facility III (Category III), twelve (12) or more workers exceeded the 54-hour average during each of the five 6-week rolling periods. Facilities I and V (Category I) also had workers who would not have met the 54-hour average limit. Facility V had by far the highest total number of individuals who did not meet the limit (108), even though the analysis for this facility only covered three 6-week rolling periods.

Table Att 2-2. Potential Violations of 10 CFR 26.205(7) (Alt. 54-Hr Limit)

Category	Facility ID	# of Instances 54-Hrs/Week Average Limit Exceeded	Max 6-Wk. Avg. Hrs/Week	# of Workers Exceeding 54-Hrs/Week Average in Each 6-Week Interval (Based on 6-Week Rolling Averages)					
				Alt. W1	Alt. W2	Alt. W3	Alt. W4	Alt. W5	Total
I	I	10	62.2	2	2	1	5	N/A	10
	V	108	62.1	33	37	38	N/A	N/A	108
III	II	3	56	1	1	0	1	0	3
	III	79	65.79	12	17	17	18	15	79
	IV	0	45.5	0	0	0	0	0	0
	VI	1	57.25	0	0	1	N/A	N/A	1
	VII	0	49.63	0	0	0	0	0	0

The NRC staff also performed descriptive statistics on the data. Table Att 2-3 shows the mean hours/week for the security officers at each facility and the hours/week of the individual at the 25th, 50th (median), and 75th percentile of the site's security officers for each week. The data provide an overview of the time distribution among security officers at these facilities. Again, note that the time unit markers (W1, W2…W10) serve only as a counting mechanism, and do not mean that the observations from all the facilities in each time unit occurred during the same calendar week. It is clear from this table that there is a temporal variation in the work hours of security officers at some facilities (for example, Facility V (Category I)) and that 25 percent or more of the security officers are working more than 54 hours per week during many weeks at Facility V (Category I) and Facility III (Category III).

Table Att 2-3. Descriptive Statistics of Hours/Week at Fuel Cycle Facility Licensees

Category			I		III				
Facility ID			I	V	II	III	IV	VI	VII
W1	Mean		38.8	47.67	21.16	42.54	40.25	39.45	34.38
	Percentiles	25%	32.0	39.00	6.00	32.42	37.43	34.00	40.00
		50%	40.1	48.00	12.00	44.83	39.00	42.00	40.00
		75%	52.0	60.25	40.00	56.92	50.28	46.50	41.00
W2	Mean		39.1	47.28	32.52	41.41	45.33	41.00	35.20
	Percentiles	25%	33.0	40.00	28.00	24.42	39.00	37.50	40.00
		50%	40.6	48.00	40.00	44.67	51.10	42.50	40.00
		75%	48.5	58.75	42.00	60.50	52.00	50.00	40.00
W3	Mean		41.5	52.93	33.74	48.50	36.98	39.25	38.03
	Percentiles	25%	38.9	45.00	28.00	37.75	29.37	37.50	40.00
		50%	41.8	53.00	42.00	56.88	39.00	42.00	40.50
		75%	51.5	66.00	42.00	61.83	39.00	45.50	47.25
W4	Mean		43.8	49.93	33.93	50.53	48.34	42.22	38.03
	Percentiles	25%	40.0	40.00	24.00	40.00	39.20	37.50	40.00
		50%	44.5	52.00	42.00	61.00	51.92	42.50	40.50
		75%	51.1	60.00	44.00	61.67	52.22	50.00	47.25

W5	Mean		42.1	46.16	34.78	48.81	39.76	41.60	40.01
	Percentiles	25%	37.5	37.50	34.00	40.00	36.98	37.50	40.00
		50%	44.0	49.00	40.00	50.92	39.00	43.00	40.00
		75%	52.5	53.25	42.00	61.42	50.62	47.00	44.00
W6	Mean		40.1	44.60	33.80	47.85	39.70	41.36	41.17
	Percentiles	25%	33.5	36.00	24.00	38.17	26.00	37.50	40.00
		50%	40.5	48.00	40.00	52.42	39.99	45.50	40.00
		75%	48.0	52.00	42.00	61.92	52.00	50.50	40.50
W7	Mean		40.0	49.00	35.59	50.35	43.02	41.15	44.27
	Percentiles	25%	33.5	40.00	36.00	45.83	39.00	37.50	43.25
		50%	40.5	52.00	40.00	60.50	45.44	42.50	44.00
		75%	48.5	57.50	42.00	61.58	52.00	50.50	48.50
W8	Mean		42.0	47.72	35.75	49.01	36.89	35.78	43.31
	Percentiles	25%	34.8	36.00	30.00	37.62	30.08	25.50	40.00
		50%	41.9	48.00	40.00	58.17	39.00	37.50	40.00
		75%	52.5	57.25	42.00	61.33	39.03	45.50	47.00
W9	Mean		42.9	31.13	35.94	48.32	44.19	N/A	41.30
	Percentiles	25%	36.5	24.00	34.00	37.50	39.00	N/A	40.00
		50%	43.0	30.25	40.00	55.83	45.43	N/A	40.00
		75%	51.0	39.50	42.00	61.50	52.00	N/A	41.00
W10	Mean		N/A	N/A	17.90	43.87	39.33	N/A	41.00
	Percentiles	25%	N/A	N/A	12.00	36.75	26.00	N/A	40.00
		50%	N/A	N/A	22.00	48.83	39.68	N/A	40.00
		75%	N/A	N/A	24.00	60.92	52.17	N/A	41.00
Facility ID			**I**	**V**	**II**	**III**	**IV**	**VI**	**VII**
Category			**I**		**III**				

Figure Att 2-1 illustrates the number of hours per week worked by the individual at the 75th percentile of the facility's security officers for each week (from Table Att 2-3). This graph shows that more than 25 percent of the security officers at Facility III (Category III) worked more than 60 hours per week in 9 out of the 10 weeks in that facility's reporting period. It also shows the variability in the weekly work hours of security personnel over the reporting period at many of the facilities included in the data set. The exceptions are Facilities II and III (both Category III), where these numbers remained relatively constant

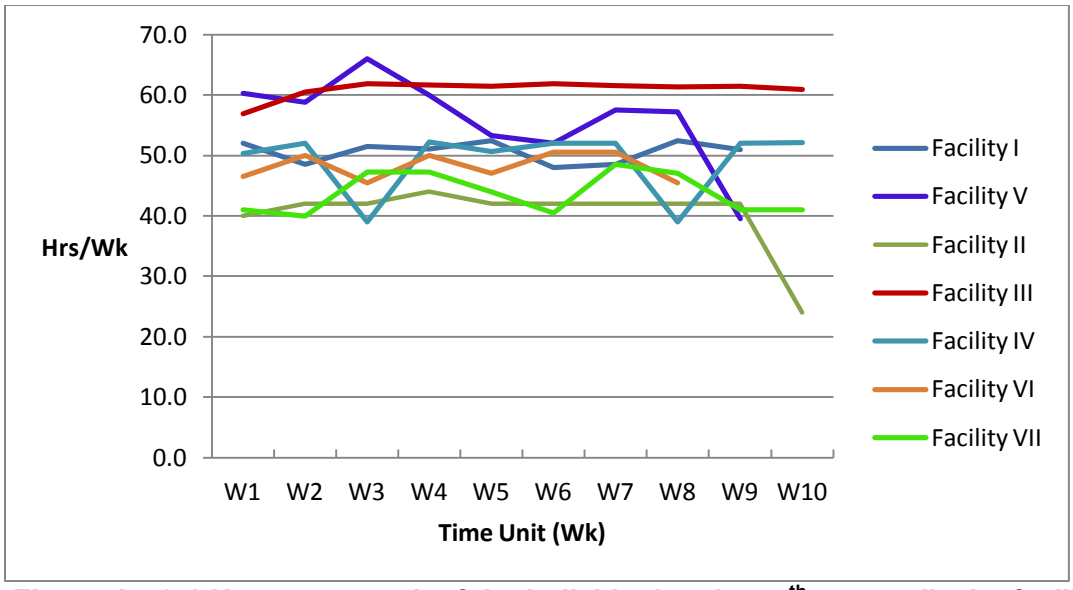

Figure Att 2-1 Hours per week of the individual at the 75th percentile, by facility and week

Table Att 2-4 lists the average number of hours worked per week by security officers as a group at each facility for each of the weeks reported. Table Att 2-5 organizes each of these weekly averages into a 10-hour-per-week bracket (for example, a weekly average of 15 hours per week would fall into the "10 to less than 20 hours per week" bracket). As seen in Table Att 2-5, most of the weekly averages for security officers at the licensees in the sample are concentrated in the 40-to-less-than-50 bracket (totaling 38) and the 30-to-less-than-40 bracket (totaling 23). There are three instances in which the weekly average of all security officers was greater than 50 hours per week, two of which occur at Facility III (Category III), and one at Facility V (Category I). At Facility II (Category III), two weekly averages were below 30 hours per week. These numbers show that the average weekly work hours for security officers as a group were well under the 72 hour-per-week limit at these facilities. However, these numbers need to be interpreted with caution. The data include many weeks in which some individuals work no (0) hours. Because of the presence of zeroes in the data set, it is possible that the inclusion of employment-status fluctuations such as resignations and new hires, as well as the possible inclusion of work by part-time employees, are reducing the reported weekly work-hour averages below the actual weekly averages for current full-time security officers at these licensees during the reporting period.

Table Att 2- 4. Weekly Average Work Hours

Time Unit	Category I		Category III				
	I	V	II	III	IV	VI	VII
W1	38.8	47.67	21.16	42.54	40.25	39.45	34.38
W2	39.1	47.28	32.52	41.41	45.33	41.00	35.20
W3	41.5	52.93	33.74	48.50	36.98	39.25	38.03
W4	43.8	49.93	33.93	50.53	48.34	42.22	38.03
W5	42.1	46.16	34.78	48.81	39.76	41.60	40.01
W6	40.1	44.60	33.80	47.85	39.70	41.36	41.17
W7	40.0	49.00	35.59	50.35	43.02	41.15	44.27
W8	42.0	47.72	35.75	49.01	36.89	35.78	43.31
W9	42.9	31.13	35.94	48.32	44.19	N/A	41.30
W10	N/A	N/A	17.90	43.87	39.33	N/A	41.00

Table Att 2-5. Weekly Average Hours Grouped Into 10-Hour Brackets

Range of Average Hours	Category I		Category III				
	I	V	II	III	IV	VI	VII
0 < - < 10	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10 ≤ - < 20	N/A	N/A	1	N/A	N/A	N/A	N/A
20 ≤ - < 30	N/A	N/A	1	N/A	N/A	N/A	N/A
30 ≤ - < 40	2	1	8	N/A	5	3	4
40 ≤ - < 50	7	7	N/A	8	5	5	6
50 ≤ - < 60	N/A	1	N/A	2	N/A	N/A	N/A
60 ≤ - < 70	N/A	N/A	N/A	N/A	N/A	N/A	N/A
70 ≤ - < 80	N/A	N/A	N/A	N/A	N/A	N/A	N/A
80 and above	N/A	N/A	N/A	N/A	N/A	N/A	N/A

To understand the individual-level work-hour patterns, the NRC staff also identified the individuals who worked in excess of 72 hours per week and those who worked in excess of 54 hours per week averaged over the rolling 6-week periods (on the basis of the 6-week rolling averages) to examine whether or not these were one-time occurrences or repeated occurrences for an individual security officer. As Table Att 2-6 demonstrates, in most cases, an individual exceeded the 72-hour threshold during only one week of the reporting period.[14] However, there were individuals who exceeded the 72-hour threshold more than once at both Category I facilities and at one of the Category III facilities. Facility V had the highest number of individuals (9) who repeatedly exceeded the 72-hour threshold on non-consecutive weeks while Facility III had the highest number of individuals (5) who worked in excess of 72 hours per week on consecutive weeks; that is, at least two weeks in a row. It is likely that the 72-hour limit was exceeded more frequently than identified in this analysis, given the rolling nature of the control.

Most individuals who exceeded the 54-hour MAWH limit at Facility I (Category I) did this only once. However, more of the individuals who exceeded this limit at Facility V (Category I) did so repeatedly (33 individuals) than those who exceeded the limit only once (14 individuals). Across facilities, most of the individuals who worked in excess of 54 hours average per week did so in consecutive 6-week periods.

Table Att 2-6. Individual-Level Analysis

Category	Facility ID	Distribution of Instances of Exceeding the 72-Hr Limit					
		Total # of instances of exceeding the threshold	# of individuals who exceeded the threshold	# of individuals exceeding the threshold only once over the reporting period	# of individuals exceeding the threshold repeatedly, but on non-consecutive weeks	# of individuals exceeding the threshold repeatedly and on consecutive weeks	Max. # of times any one individual exceeded the threshold during the reporting period
I	I	5	4	3 (75%)	0 (0%)	1 (25%)	2
	V	68	55	45 (82%)	9 (16%)	1 (2%)	3
III	II	2	2	2 (100%)	0 (0%)	0 (0%)	1

[14] Note that the 72-hours-in-7-days limit is a rolling limit. Because the data for this analysis were total hours per week (not hourly or daily) data, these results may underestimate the number of times the limit was exceeded.

	III	26	19	13 (68%)	1 (5%)	5 (26%)	3
	IV	0	0	0	0	0	0
	VI	0	0	0	0	0	0
	VII	0	0	0	0	0	0
Category	**Facility ID**	**Distribution of Instances of Exceeding the 54-Hr Limit**					
		Total # of instances of exceeding the threshold	**# of individuals who exceeded the threshold**	**# of individuals exceeding the threshold only once over the reporting period**	**# of individuals exceeding the threshold repeatedly, but in non-consecutive 6-week periods**	**# of individuals exceeding the threshold repeatedly and in consecutive 6-week periods**	**Max. # of times any one individual exceeded the threshold during the reporting period**
I	I	10	6	4 (68%)	1 (17%)	1 (17%)	4
	V	108	50	14 (28%)	3 (6%)	33 (66%)	3
III	II	3	2	1 (50%)	0 (0%)	1 (50%)	2
	III	79	20	2 (10%)	0 (0%)	18 (90%)	5
	IV	0	0	0	0	0	0
	VI	1	1	1 (100%)	0 (0%)	0 (0%)	1
	VII	0	0	0	0	0	0

The data from the two-month survey strengthens staff's concern that the work schedules at Facility V (a Category I facility) might have subjected security officers to acute and cumulative fatigue. While Facility V has a written policy in place stating that security officers shall not exceed 60 hours per week unless approved by the Security management, the data shows that this exemption was applied on many occasions.

Although some of these facilities do an adequate job in controlling their security officers' work hours at the individual and group levels, this does not guarantee that these facilities will continue to satisfactorily control their security officers' work hours in the future. Some of these facilities, like Facility V, have a written policy in place to control fatigue/security officer work hours, but as in the case of Facility V, the policy allows management to exceed administrative controls on many occasions to support facility operations.

Attachment 3 – Category I: Fixed Site Physical Protection Requirements

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)]

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. [73.60(f)]

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]

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.

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

Licensee should establish, maintain, and implement an insider mitigation program and shall 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 the site corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the physical protection program. [1]

Implementation of security plans and associated procedures should be coordinated with other onsite plans and procedures to preclude conflict during both normal and 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)]

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), 73.46(b)(4)]

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]

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

Bullet resistant barriers

The central alarm station, and the location within which the last access control function for access to the protected area is performed, should be bullet-resisting.

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.

Isolation zone

An isolation zone should be maintained in outdoor areas adjacent to the protected area perimeter barrier. The isolation zone should be designed of and sufficient size to permit observation and assessment of activities on either side of the protected area barrier. [73.46(c)(3)]

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 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.

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.

Unoccupied vital areas should be locked and alarmed.

At a minimum, the following shall be considered vital areas: (1) central alarm station; and (2) secondary alarm station.

At a minimum, the following shall 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 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.

High enriched uranium, plutonium or uranium-233 should be processed and stored within a material access area. More than one material access area may be located within a single protected area. [73.46(c)(1), 73.46(c)(5)]

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 within a material access area 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 or under the control of at least two authorized individuals. [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 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. [73.46(c)(1) - 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 serveilled 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. Water approaches should be periodically surveilled and observed. [2]

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), 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 no less frequently than every 31 days. [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 an armed member of the security organization. [73.46(d)(8)]

Vital Areas

Licensees should control access into vital areas consistent with access authorization lists.

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)(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 individuals (two person rule). [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 that 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 employ 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.

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)]

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. Only authorized and confirmed forms and amounts of high enriched uranium, plutonium or uranium-233 should be removed from material access areas. [73.46(d)(4), 73.45(e), 2]

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. 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. A third trained and equipped security personnel should provide over-watch of the vehicle search. [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)(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]

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)]

Federal, State and local law enforcement personnel on official duty and U.S. Department of Energy couriers engaged in transporting SNM are excepted from search requirements. [73.46(d)(4)] 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 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. [73.46(d)(9)]

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)]

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

Search for firearms, 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 search at vehicle access portals to include searching the cab, engine compartment, under carriage and cargo areas.

Federal, State and local law enforcement personnel on official duty and U.S. Department of Energy personnel engaged in transporting SNM are excepted from search requirements. Armed security officers who are on duty and have exited the material access area may re-enter the protected area without being searched for firearms.

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 individuals who are not authorized access to that material access area. [73.46(d)(9)]

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

Containers of contaminated wastes should be drum scanned and tamper sealed by at least two individuals who are not authorized access to material processing and storage areas. [73.46(d)(10)]

Licensees should search all individuals entering vaults for weapons. [2]

<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)]

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 members tactical response team. [73.46(e)(4)]

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)(7)]

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)]

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 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 periodically checked to detect and deter unauthorized personnel, vehicles and materials.

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. [73.46(e)(8), 2]

Methods to continuously observe individuals within material access areas should be provided 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)(4)]

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]

Alarm station operators should be capable of calling for assistance in accordance with security plans and implementing procedures. [73.46(f)(1)]

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 within pre-determined time lines 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 ten. [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 documents 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]

<u>Security Program Review</u>

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 audible form and available for inspection. [73.46(g)(6)]

Findings from these reviews should be entered into the site corrective action program, if present.

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 in the site corrective action program or security event log. [73.46(g)(5)]

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.

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, retain, and remove 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 Requirements

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 and should describe the program in the Physical Security Plan.

Licensees should use the site corrective action or security event log program 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 both normal and 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.

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 processed and stored within a protected area within a controlled access area.

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

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.

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 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 serveilled 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. 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. In addition, a licensee's access authorization program should include the requirements in §73.57, §73.59 and §73.61.

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 an armed 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 that 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 employ 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.

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.

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 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 stations 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 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 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.

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.

<u>Security Program Review</u>

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.

Findings from these reviews should be entered into the site corrective action program, if present.

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 in the site corrective action program or security event log.

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, retain, and remove 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 Requirements

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 shall 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.

Licensee should use the site corrective action program or security event log 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 both normal and 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 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 that 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 employ 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, at all times, 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.

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 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 audible form and available for inspection.

Findings from these reviews should be entered into the site corrective action program, if present.

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, retain, and remove 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 Requirements

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]

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 the site corrective action program or security event log 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 both normal and 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. [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 processed and stored within protected area within a controlled access area.

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

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 of and sufficient size to permit observation and assessment of activities on either side of the protected area barrier.

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 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 serveilled 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. 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)] In addition, a licensee's access authorization program should include the requirements in §73.57, §73.59 and §73.61.

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 an armed 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 that 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 employ 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)(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 stations 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 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.

<u>Security Program Review</u>

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 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.

Findings from these reviews should be entered into the site corrective action program, if present.

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 in the site corrective action program or security event log.

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, retain, and remove 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 Requirements

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 the site corrective action program or security event log 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 both normal and 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 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. 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.

Category II - moderately dilute SNM should be processed and stored within a controlled access area.

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

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.

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 protected areas and security systems to reduce the probability of compromise.

Access control devices should only be issued to individuals with unescorted access that 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 employ 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.

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

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 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 stations 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 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 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.

<u>Communication</u>

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.

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 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.

Findings from these reviews should be entered into the site corrective action program, if present.

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 in the site corrective action program or security event log.

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, retain, and remove 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 Requirements

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 shall 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 III SNM. [1]

Licensee should use the site corrective action program or security event log 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 both normal and emergency conditions. [1]

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 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.

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 member 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 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.

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 processed and stored within a controlled access area. [73.67(f)(1) – 73.67(d)(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. [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, 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. [73.67(d)(4)]

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 that 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 employ 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. [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. [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. [73.67(d)(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 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(d)(3)]

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, at all times, in accordance with security plans and implementing procedures. [73.67(d)(9)] 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.

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 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 audible form and available for inspection.

Findings from these reviews should be entered into the site corrective action program, if present.

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, retain, and remove 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 Requirements for Category III Plutonium and Small Quantities of Spent Nuclear Fuel

In addition to the Category III physical protection requirements for theft or diversion, licensees that possess Category III quantities of plutonium and less than 100 grams of spent nuclear fuel should implement the following requirements.

Access Authorization

A licensee's access authorization program should include the requirements in 10 CFR 73.57.

Detection and Assessment

Licensees should establish and maintain the capability to continuously monitor and detect without delay all unauthorized entries into areas containing plutonium. (Note, this may be the entire controlled access area or another controlled access area specifically for plutonium)

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 is linked to an onsite or offsite central monitoring facility; or
2. Electronic devices 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.

Attachment 10 – Category I: Transportation Physical Protection Requirements

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 shall 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 use the corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

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

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 of 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 of 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 vehiclesshould 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.

Export/import shipments

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 exports 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

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, 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 in the site corrective action program or security event log. [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.

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, retain, and remove 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 Requirements

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 the corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program. Implementation of transportation security plans and associated procedures should be coordinated with other plans and procedures to preclude conflict during both normal and emergency conditions.

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 of 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 of 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.

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:

> (i) 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.
>
> (ii) 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 exports 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

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, 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 in the site corrective action program or security event log.

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.

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, retain, and remove 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 Requirements

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.

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 highly-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. However, no NRC-conducted force-on-force exercises are required.

Licensees should use the corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

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

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.

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

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 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

Licensees should control access to SNM loading and transfer areas, a conveyance and containers where Category III material is located 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 limit unescorted access to the controlled access areas, transports, 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.

Export and Import Shipments

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 exports Category I highly-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

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, 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.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance and testing 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.

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.

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, retain, and remove 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.

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 2000 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, during intermodal transfers, and upon arrival.

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.
- Arrange for the in-transit physical protection of the materials unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection.

Reciever 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,
- Notify the shipper of receipt of the material, and
- Arrange for the in-transit physical protection of the material unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection.

Carrier requirements

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 shall 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, and

- 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.

Attachment 13 – Category II: Transportation Physical Protection Requirements

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. However, no NRC-conducted force-on-force exercises are required.

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)]

Licensee should establish, maintain, and implement an insider mitigation program and shall 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 use the corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

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

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. [73.67(e)(1)]

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 of 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 of 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)and 73.67(e)(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.

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 imports or exports 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 exports 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

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, 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 in the site corrective action program or security event log.

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.

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 [73.67(e)(4)]

The NRC may inspect, copy, retain, and remove 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 en 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 Requirements

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.

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 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. 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 Physical Security Plan.

Licensees should use the corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

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

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 should include 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.

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

Licensees should control access to SNM loading and transfer areas, a conveyance and containers where Category II moderately-dilute material is located 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 limit unescorted access to the controlled access areas, transports, 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.

Personnel Trustworthiness

Licensee should establish, maintain, and implement a personnel trustworthiness program and shall 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.

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 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 exports Category II 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

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, 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.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance and testing 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.

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.

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, retain, and remove 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.

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 2000 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, during intermodal transfers, and upon arrival.

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.
- Arrange for the in-transit physical protection of the materials unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection.

Reciever 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,
- Notify the shipper of receipt of the material, and
- Arrange for the in-transit physical protection of the material unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection.

Carrier requirements

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. The licensee shall 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, and

- 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 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 shall comply with the requirements of this section. The licensee shall 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.

Orders regarding simultaneous shipments

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 en 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 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.

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 III 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. However, no NRC-conducted force-on-force exercises are required.

Licensees should use the corrective action program or security event log to track, trend, correct and prevent recurrence of failures and deficiencies in the transportation security program.

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

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.

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

Licensees should establish, maintain, and implement an access authorization program and should describe the program in the Transportation Security Plan.

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 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

Licensees should control access to SNM loading and transfer areas, a conveyance and containers where Category III material is located 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 limit unescorted access to the controlled access areas, transports, 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.

Export and Import Shipments

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 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 exports Category III 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. [73.67(g)(4)]

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, 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.

Maintenance and Testing

Performance capabilities

Licensees should establish, maintain and implement a maintenance and testing 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.

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.

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, retain, and remove 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.

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 2000 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.

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.

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.
- 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.
- Arrange for the in-transit physical protection of the materials unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection. [73.67(g)(1)]

Receiver requirements

(2) Each licensee who receives Category III SNM should:

- Immediately accept the shipment upon arrival.
- Check the integrity of the locks, containers and seals upon receipt of the shipment,
- Notify the shipper of receipt of the material, and
- Arrange for the in-transit physical protection of the material in accordance with the requirements of [§ 73.67(g)(3)] unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection. [73.67(g)(2)]

Carrier requirements

(3) 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.
- Establish and maintain written response procedures for dealing with threats of thefts or thefts or sabotage of this material. The licensee shall 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, and
- 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. [73.67(g)(3)]