POLICY ISSUE
(Notation Vote)

August 28, 2007 SECY-07-0148

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations **/RA/**

SUBJECT: INDEPENDENT SPENT FUEL STORAGE INSTALLATION SECURITY REQUIREMENTS FOR RADIOLOGICAL SABOTAGE

PURPOSE:

To obtain Commission direction on policy issues necessary for the development of an upcoming proposed rulemaking on independent spent fuel storage installation (ISFSI) security requirements.

SUMMARY:

This paper provides a comprehensive evaluation of the current regulatory basis for ISFSI security requirements, identifies six policy issues requiring U.S. Nuclear Regulatory Commission (Commission or NRC) direction, and provides options and recommendations for the Commission's consideration. The outcome of these policy issues will inform an upcoming proposed ISFSI security rulemaking. This rulemaking is intended to: update the regulations to support the current regulatory environment, address insights gained from the ISFSI security assessments, apply a consistent approach across all ISFSIs irrespective of their license type or location, and resolve ISFSI security issues (e.g., applicability of the design basis threat (DBT) for radiological sabotage to ISFSIs). The Commission previously approved the accomplishment of the upcoming proposed ISFSI security rulemaking in Staff Requirements Memorandum (SRM)-COMSECY-05-0058.[1]

[1] COMSECY-05-0058, "Schedules and Resources for Security Rulemakings," Agencywide Documents Access and Management System (ADAMS) No. ML052990371, dated November 16, 2005.

CONTACTS: Philip Brochman, NSIR/DSP
(301) 415-6557

Shana Helton, NMSS/SFST
(301) 492-3284

Upon separation of Enclosure 6, this document is ~~**OFFICIAL USE ONLY - SECURITY-RELATED INFORMATION**~~, ~~until and unless the Commission determines otherwise~~ **DECONTROLLED**.

In this paper, the staff examines options for several policy issues. Specifically, the staff is recommending the development of new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements. These new security requirements, which would be informed by the existing ISFSI orders and by recent changes to the DBT for radiological sabotage, would establish a dose limit for security scenarios for ISFSIs that is consistent with the Commission assumptions and current dose limits for safety-related design basis accidents. To increase stakeholder understanding of these ISFSI security issues and participation in the proposed rulemaking, the staff recommends publicly releasing this paper along with redacted portions of Enclosures 1 through 5.

Enclosures 1 through 4 contain detailed analyses of Policy Issues 1 through 4, respectively. Enclosure 5 contains supplemental background information on threat assessments and the CARVER-type analysis methodology referenced in Policy Issue 3. Enclosure 6 contains additional Safeguards Information developed in response to questions raised by the Commission at the staff's April 3, 2006, briefing on ISFSI security issues and licensing actions.

The goals of the upcoming proposed ISFSI security rulemaking include: (1) making generically applicable the requirements similar to those imposed by the October 2002 ISFSI security orders; (2) ensuring that a consistent overall protective strategy is maintained for all ISFSIs; (3) incorporating the direction on the policy issues discussed in this paper; and (4) incorporating any necessary conforming changes to the ISFSI licensing, security, and emergency planning requirements. The resource implications for the options and the out year implementation costs are described in the Resources section.

BACKGROUND:

The current ISFSI security regulatory structure is complex to many staff, licensees, and the public and thus does not meet the NRC's objective of regulatory clarity. This complexity is due to multiple factors, including: the different types of ISFSI licenses (both general and specific licenses); differing impacts and applicability of regulations (based upon whether the ISFSI is collocated with an operating power reactor, collocated with a decommissioning power reactor, or is located away from any power reactors); previous staff practices in applying security requirements; staff recommendations to defer addressing ISFSI issues in the April 2003 DBT orders and the subsequent DBT rulemaking; and the length of time since ISFSI security regulations were substantively updated.

Following the events of September 11, 2001, the NRC issued security orders in October 2002 to all ISFSI licensees, regardless of the ISFSI type.[2] ISFSI licensees were not, however, included within the scope of the April 2003 DBT orders issued to power reactor licensees. While the current regulations for ISFSI security differ depending on license type and location of the ISFSI, the ISFSI security orders ensured that a consistent overall protective strategy is in place for all ISFSIs. The proposed ISFSI security rulemaking would update the regulations and make the

[2] See *Federal Register* notices 67 FR 65150 and 67 FR 65152, dated October 23, 2002.

ISFSI security orders generically applicable to all ISFSI licensees, regardless of the type of license and the location of the ISFSI.

In addition to the security orders, the staff completed security assessments for several types of ISFSI storage cask designs. The staff informed the Commission of the results of this security assessment for spent fuel storage casks and transportation packages in SECY-06-0045.[3] The proposed ISFSI security rulemaking would address long-term issues raised by the security assessment and other ISFSI regulatory issues. Separately, the staff briefed the Commission on April 3, 2006, on ISFSI security issues and licensing actions. As a result of that briefing, the staff was asked to address three issues related to ISFSI security, which pertained to particular sites. The staff provided a Note to the Commissioners' Assistants on May 16, 2006,[4] which partially addressed the issues raised in the Commission briefing. Enclosure 6 to this paper clarifies and completes the staff's response to the Commission on these three remaining issues.

As the staff responded to the Commission's questions and began to analyze the regulatory and policy issues associated with the proposed ISFSI security rulemaking, a number of new policy issues arose for which early Commission direction is sought. In particular, the staff identified several questions on a number of differences between the current security regulations for the different types of ISFSI licensees. These differences do not pose an urgent safety or security concern because the ISFSI security orders issued subsequent to the events of September 11, 2001, ensure that all ISFSI licensees have the same level of protection. One of the differences in the regulations arose due to the scope of the recently completed final DBT rule,[5] which was limited to power reactors and to Category I special nuclear material licensees. Therefore, the staff recommended deferring resolution of issues on the consistent application of the DBT for radiological sabotage to all ISFSI licensees to a future ISFSI security rulemaking.[6] The proposed and final DBT rules were provided to the Commission in SECY-05-0106 and SECY-06-0219, respectively.[7]

Under 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-Level Radioactive Waste, and Reactor-Related Greater than Class C Waste," there are two types of ISFSI licenses (i.e., general and specific) that are available for the storage of

---

[3] SECY-06-0045, "Results of Implementation of the Decisionmaking Framework for Materials and Research and Test Reactor Security Assessments," ADAMS No. ML060340452, dated March 1, 2006.

[4] Note to the Commissioners' Assistants, "Response to Commissioner McGaffigan on Independent Spent Fuel Storage Installations (ISFSI) Security," ADAMS No. ML061370015, dated May 16, 2006.

[5] Final Rule - 10 CFR Part 73, "Design Basis Threat." Published in the *Federal Register* (72 FR 12705) on March 19, 2007.

[6] See previous *Federal Register* notice 72 FR 12705, public comment Issue 5 (at 72 FR 12716).

[7] SECY-05-0106, "Proposed Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements," ADAMS No. ML050530088, dated June 14, 2005. SECY-06-0219, "Final Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements," ADAMS No. ML062130289, dated October 30, 2006.

spent fuel. Physical security requirements are located in various sections in 10 CFR Part 73, "Physical Protection of Plants and Materials," depending on the type of licensee. Additionally, the regulations in 10 CFR 72.212(b)(5), "Conditions of General License Issued under § 72.210," require general licensees to establish a physical protection program that protects the spent fuel against the DBT for radiological sabotage in accordance with 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage." For general-license ISFSIs, neither 10 CFR 72.212(b)(5) nor 10 CFR 73.55 impose a dose limit for security events (i.e., acts of radiological sabotage). For certain specific license-ISFSIs, 10 CFR 72.106 does specify a 0.05-Sv (5-rem) dose limit for both safety-related and security-related events.[8]

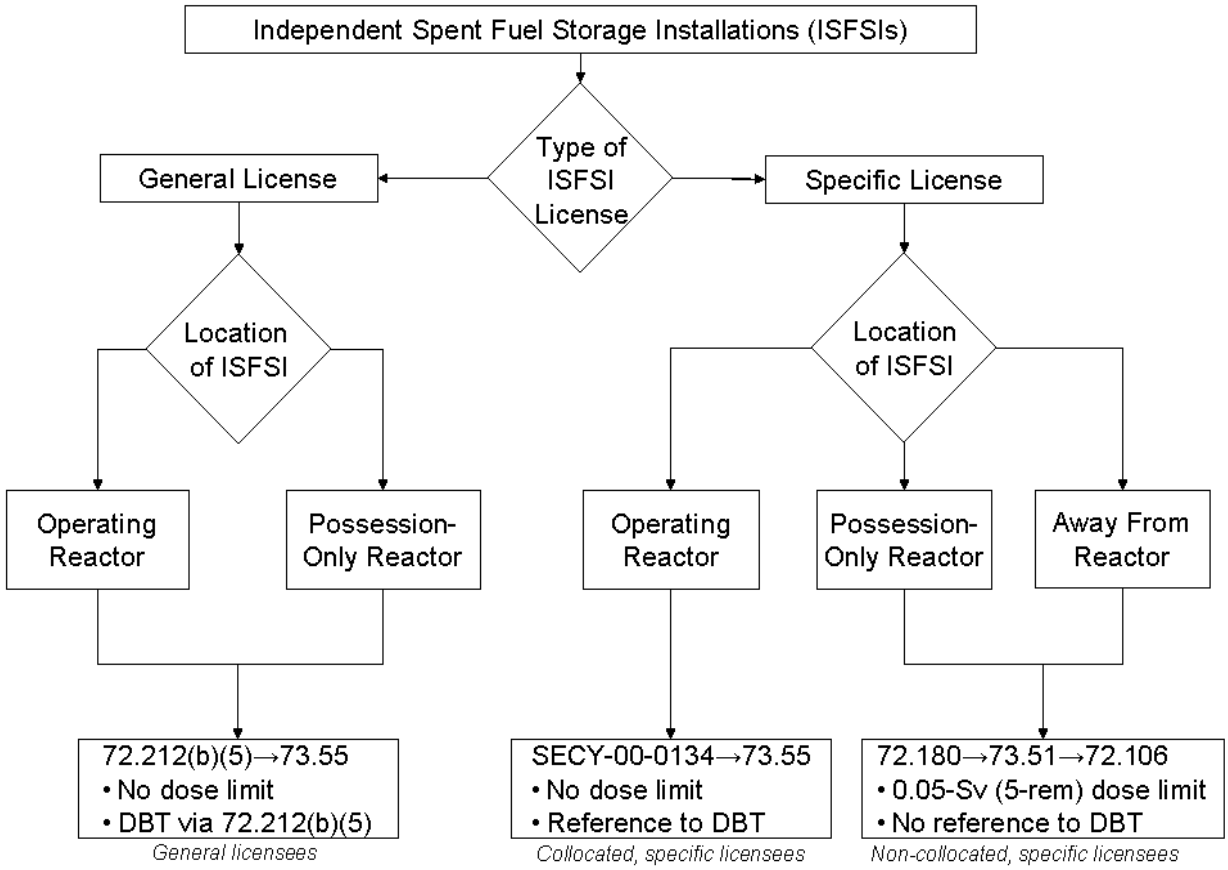

Figure 1 - Governing regulations for ISFSI security requirements

[8] The dose criteria in Title 10 of the *Code of Federal Regulations* (CFR) 72.106, "Controlled area of an ISFSI or MRS," (0.05 Sievert (Sv) [5 rem] total effective dose equivalent; 0.15 Sv [15 rem] to the lens of the eye; 0.5 Sv [50 rem] as either the sum of the deep dose equivalent and any organ dose, or the shallow dose equivalent to the skin or any extremity) are hereinafter referred to as the 0.05-Sv (5-rem) dose limit.

The staff has developed the above figure (Figure 1) as an aid in describing the applicability of the current ISFSI licensing and security regulations under 10 CFR Parts 72 and 73, respectively.

Based on their applicability provisions, 10 CFR 72.180, "Physical Protection Plan," and 10 CFR 73.51, "Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-level Radioactive Waste," apply to all specific-license ISFSIs without any options. However, past staff practice has permitted collocated, specific licensees[9] to develop their ISFSI's security plans based upon on the requirements of 10 CFR 73.55.[10] Additionally, the statements of consideration accompanying a Part 72 final rule[11] clarifying the applicability of the various provisions of Part 72 to general licensees, specific licensees, and certificate holders indicated that specific licensees collocated at an operating 10 CFR Part 50 ("Domestic Licensing of Production and Utilization Facilities") power reactor facility are excluded from the provisions of 10 CFR 73.51. Therefore, in practice, the staff has only subjected non-collocated, specific licensees to the requirements of 10 CFR 72.180, which states such licensees must establish, maintain, and implement a detailed plan for physical protection as described in 10 CFR 73.51.

The regulations in 10 CFR 73.51 require non-collocated, specific licensees to have a physical protection system that is designed such that a loss of control of the facility (e.g., from a terrorist attack) would not result in a radiation exposure exceeding a 0.05-Sv (5-rem) dose limit at the controlled area boundary (the safety dose limits of 10 CFR 72.106). Unlike the regulations in 10 CFR 72.212(b)(5), neither 10 CFR 72.180 nor 73.51 includes specific language requiring a specific ISFSI licensee to protect the spent fuel or high-level radioactive waste against the DBT for radiological sabotage. Additionally, the scope of the recent final rule revising the DBT for radiological sabotage (10 CFR 73.1, "Purpose and scope") was silent on specific-license ISFSIs (i.e., it did not specifically exclude such a class of licensees). In fact, 10 CFR 73.1 lists exceptions to certain DBT requirements for various classes of licensees. Specific-license ISFSIs had previously been identified as being exempted from certain provisions of the DBT rule, but were removed by staff in this most recent final rule. This was because 10 CFR 72.180 did not contain specific language requiring protection of the spent fuel (in a specific-license

[9] For the purposes of this paper, the staff will use the term "collocated, specific licensee" to mean a specific-license ISFSI that is collocated at a power reactor facility which has a license to operate. The term "non-collocated, specific licensee" will include both a specific-license ISFSI that is collocated with a power reactor with a possession-only license and a specific-license ISFSI located away from any power reactors. This nomenclature is reflected in Figure 1.

[10] Letter to Mr. James P. O'Hanlon, "Request for Exemption from 10 CFR 73.51(d)(3) Requirements, North Anna Independent Spent Fuel Storage Installation (ISFSI) and Surry ISFSI (TAC Nos. L22707 and L22708)," ADAMS No. ML060320261, dated November 12, 1998.

[11] Final Rule - 10 CFR Part 72, "Clarification and Addition of Flexibility." Published in the *Federal Register* (65 FR 50606) on August 21, 2000. See public comment Issue A.1.

ISFSI) against the DBT for radiological sabotage[12] (i.e., the intent of the rule was for 10 CFR 73.1 to remain consistent with 10 CFR 72.180). Consequently, the current regulations are inconsistent and do not specify whether collocated, specific-license ISFSIs are required to protect against the DBT for radiological sabotage, in contrast to the clear requirement for general-license ISFSIs under 10 CFR 72.212(b)(5).

Even though both general and collocated, specific licensees are required to comply with selected provisions of 10 CFR 73.55, the proposed power reactor security rule revising this regulation does not address security requirements for collocated, specific-license ISFSIs. The Commission approved the staff's proposed rule in SRM-SECY-06-0126.[13] The staff considered inclusion of ISFSI security requirements as beyond the scope of the proposed power reactor security rule, since the rule was focused on making generically applicable reactor security requirements previously imposed by Commission order and on other agency power reactor security initiatives.

Finally, staff notes that conservatisms may exist in the modeling of the quantity of radiological material that might be released from an attack against spent fuel in a storage cask (i.e., the release fraction). Consequently, staff embarked on a study of this issue in conjunction with several other countries and the U.S. Department of Energy (DOE). This study would perform experimental validation of release fractions using actual spent fuel. Additionally, staff is working with DOE and the U.S. Department of State to establish a multilateral agreement with these countries to permit the multilateral sharing of classified information on this topic that currently exists in these countries and the U.S. While these projects have been underway for several years, the staff does not expect to complete these efforts in time to provide input into the development of the technical bases for the proposed ISFSI security rulemaking. However, the results of these studies would be expected to be reflected in regulatory guidance documents supporting a final rule. Therefore, the status of these issues should not delay this proposed ISFSI security rule.

DISCUSSION:

One of the staff's major goals of the proposed ISFSI security rulemaking is to clarify the applicability of the ISFSI security requirements in 10 CFR Part 73 for both general-license and specific-license ISFSIs. A second goal is to make requirements similar to those imposed by the ISFSI security orders generically applicable to all ISFSI licensees. Accordingly, before beginning development of the technical bases supporting the ISFSI security rulemaking, the staff seeks early Commission direction on the following six policy issues. The staff has not engaged any external stakeholders in developing this paper. As an aid to reviewing this paper,

---

[12] See previous *Federal Register* notice 72 FR 12705, public comment Issue 5 (at 72 FR 12716).

[13] SECY-06-0126, "Proposed Rulemaking - Power Reactor Security Requirements," ADAMS No. ML00830634, dated May 31, 2006. Approved by SRM-SECY-06-0126, ADAMS No. ML061840301, dated June 30, 2006. Published for comment in the *Federal Register* (72 FR 62663) on October 26, 2006.

the staff notes the discussions in the later policy issues build upon the staff's recommendations from the previous policy issues.

The staff anticipates that this rulemaking is likely to raise certain backfitting issues under 10 CFR 72.62, "Backfitting." The staff has not performed a backfit analysis for the various options under these six policy issues. Informed by the Commission's direction on these policy issues, the staff would perform a backfit analysis and cost assessment as part of the development of the proposed rule. In the interim, the staff has provided a rough assessment of potential licensee costs in the Schedule and Impacts section of this paper.

Issue 1: Should a radiological acceptance criterion for security scenarios be applied consistently to all ISFSIs?

Specific-license ISFSIs are currently required by 10 CFR 73.51 to meet a 0.05-Sv (5-rem) dose limit (see footnote 8) for acts of radiological sabotage. However, the current regulations do not specify an explicit dose limit for security (radiological sabotage) events for general-license ISFSIs. The staff has historically considered general licensees—which are required by 10 CFR 72.212(b)(v) to protect the spent nuclear fuel against the DBT of radiological sabotage—to have the same level of protection as required for specific licensees.

Policy Issue 1 and its options are discussed in more detail in Enclosure 1. The staff has identified four options for Policy Issue 1:

1. Retain the current dose limits and clarify the applicability of the ISFSI security requirements.

2. Eliminate the radiological dose criterion for all ISFSIs and apply the current protective strategy, which includes the security orders.

3. Eliminate the radiological dose criterion for all ISFSIs and require ISFSI licensees to prevent or impede attempted acts of radiological sabotage.

4. Apply the radiological dose criterion to all ISFSIs.

   (a) The staff performs the assessments to determine whether the ISFSI is in compliance with the dose limit; or

   (b) The licensee performs the assessments and demonstrates that the ISFSI is in compliance with the dose limit.

The staff recommends Option 4(b). This option is performance-based, and affords the ISFSI licensee the greatest amount of flexibility in meeting the regulations. This option is consistent with the historic NRC regulatory model requiring licensees to demonstrate compliance, and minimizes licensee fee costs and the impact on staff resources. Additionally, this option provides consistency for the differing types of ISFSI licensees, and also provides a metric that is independent of future fuel loading characteristics and dry-cask storage designs. The licensee's

assessments that their ISFSI was in compliance with the dose limits would be subject to review and/or inspection by the staff, as appropriate. The following paragraphs provide a brief assessment of some of the potential implications and impacts on ISFSI licensing and inspection programs that may arise from this policy option. A fuller discussion of these issues is provided in Enclosure 1.

Under a dose-based acceptance criteria, some ISFSI licensees might have to revise their current protective strategy from a "detect, assess, and communicate" protective strategy to a "denial of task" protective strategy due to site-specific limitations (e.g., limited room to expand the distance between their ISFSI and their controlled area boundary). Consequently, if a constrained licensee cannot meet the dose limit through the use of passive security measures (e.g., the use of engineered security features or through changes to the ISFSI's design), one of the options available to the licensee would be to use active security measures (e.g., a "denial" protective strategy) to prevent a successful terrorist attack. The staff envisions that only very few licensees may be sufficiently constrained to be unable to meet the radiological dose criterion through the use of passive security measures and thus would be compelled to shift to a "denial of task" protective strategy. Moreover, the staff recommends continuing the current practice of not performing force-on-force (FOF) exercises against ISFSIs. However, if an ISFSI licensee revises its security program to employ a "denial of task" protective strategy, then the staff would reevaluate the need for a FOF exercise against that ISFSI on a case-by-case basis.

The use of a "denial of task" protective strategy raises issues of sufficient technical complexity to necessitate prior staff review and approval of a licensee's security plan. The staff bases this conclusion on: (1) experience gained in the CY 2003 - CY 2004 reviews of changes to reactor security plans to implement the security and DBT orders and the resultant degree of complexity and the need for interactions with licensees; and (2) a desire to maintain an appropriate independence and separation of NRC security plan review and approval and inspection functions. For a specific-license ISFSI, NRC prior review and approval of applicant's initial security plans is required under the current regulations. Under 10 CFR 72.44(e), "License Conditions," licensees may make certain changes to their security plan without NRC prior review and approval, if such changes do not decrease the effectiveness of the security plan. For a general-license ISFSI, the security requirements for the ISFSI are incorporated in the security plan (required under Part 50) for the associated power reactor license and are subject to inspection by NRC regional staff, not to staff prior review and approval. Similarly, reactor licensees are permitted under 10 CFR 50.54(p)(1), "Conditions of Licenses," to make certain changes to their security plan without prior NRC review and approval, provided such changes do not decrease the effectiveness of their security plan. In all likelihood, a general-license ISFSI's shift to a denial protective strategy would not decrease the effectiveness of the associated power reactor's security plan under 10 CFR 50.54(p)(1). However, as discussed earlier and notwithstanding the provisions of 10 CFR 50.54(p)(1), the staff would revise the regulations to require a reactor licensee, associated with a general-license ISFSI who chooses to employ a "denial of task" protective strategy for the ISFSI, to submit its security plan (for protecting both the reactor and ISFSI) to the NRC for prior review and approval. The NRC's

approval of a revised security plan for the site would be a specific licensing action under the Part 50 license that would create a potential hearing right.[14]

However, the staff notes that some Part 50 licenses who are currently using the Part 72 general license process have required amendments to their Part 50 license to accommodate the presence of the ISFSI, thus creating a potential hearing right under the Part 50 license. An example of this was for heavy loads issues (e.g., the use of single failure proof cranes and revised heavy load pathways). Therefore, revising the necessary regulations to require a general-license ISFSI, who was compelled to adopt a "denial of task" protective strategy, to submit the site (reactor and ISFSI) security plan to the NRC for review and approval would be consistent with the current Part 50 reactor license/Part 72 general-license ISFSI regulations. Consequently, the staff's view is that the potential for hearing requests would be essentially the same as it is under the current regulations.

Issue 2: Should the dose limits for acts of radiological sabotage (if any are established under Policy Issue 1) be the same as the dose limits for design-basis accidents?

In the current regulations, the dose limit for security scenarios for non-collocated, specific-license ISFSIs is consistent with the dose limit for design basis accidents (DBAs) of 0.05 Sv (5-rem) at the controlled area boundary. As discussed in the statements of consideration accompanying the final rule initially promulgating 10 CFR Part 72,[15] this dose limit was derived from protective actions recommended by the U.S. Environmental Protection Agency (EPA) for projected doses to populations for planning purposes. Additionally, an NRC 1995 ISFSI emergency planning final rule indicated that a release exceeding the EPA Protective Action Guidelines (PAGs) would not occur;[16] consequently, no verification was required that doses would be less than a 0.01-Sv (1-rem) dose limit at the site area boundary. Accordingly, if the Commission determines, under Policy Issue 1, that a radiological acceptance criterion for acts of radiological sabotage should be applied to all ISFSI licensees, is a 0.05-Sv (5-rem) dose limit criteria still the appropriate limit?

---

[14] The current Part 72 general license regulations implement provisions of Section 218(a) of the Nuclear Waste Policy Act of 1982, as amended (42 U.S.C. 10198), that mandated that the Commission by rule approve technologies for the dry storage of spent fuel at civilian nuclear power reactors, "without to the extent practicable," the need for additional site specific [licensing] approvals by the Commission. Under the current Part 72 general license regulations, no site-specific licensing actions are required to use dry storage casks to store spent fuel.

[15] Final rule - 10 CFR Part 72, "Licensing Requirements for the Storage of Spent Fuel In an Independent Fuel Spent Storage Installation." Published in the *Federal Register* (45 FR 74693) on November 12, 1980. See public comment Issues 20 and 21 (at 45 FR 74696 and 74697).

[16] Final rule - 10 CFR Part 72, "Emergency Planning Licensing Requirements for Independent Spent Fuel Storage Facilities (ISFSI) and Monitored Retrievable Storage Facilities (MRS)." Published in the *Federal Register* (60 FR 32430) on June 22, 1995. See public comment Issues 17 and 25 (at 60 FR 32434 and 32435).

Policy Issue 2 and its options are discussed in more detail in Enclosure 2. The staff has identified four options for Policy Issue 2:

1. Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary).

2. Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary); and also meet a 0.01-Sv (1-rem) dose limit for both safety and security events at the site area boundary.

3. Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., 0.05 Sv (5 rem)), but apply it at the site area boundary instead of at the controlled area boundary. (Changes to ISFSI emergency planning requirements—i.e., the potential to classify events to a "general emergency" level-would likely be required.)

4. Increase the dose limit for radiological sabotage consistent with the dose limit for reactor DBAs (i.e., 0.25 Sv (25 rem) at the site area boundary). (Changes to ISFSI emergency planning requirements—i.e., the potential to classify events to a "general emergency" level—would be required.)

The staff recommends Option 2. This option provides consistency between the dose limits for ISFSI DBAs and acts of radiological sabotage. Since this paper contemplates ISFSI licensees potentially extending their controlled area boundary outward (to meet a radiological sabotage dose limit), the staff would propose adding a new requirement for licensees to verify doses are also less than 0.01 Sv (1 rem) at the site boundary. The term "site boundary" is defined in 10 CFR 20.1003 ("Definitions"); however, it is not defined in 10 CFR Part 72 or Part 73. Given the differences in the physical location of an ISFSI at the various reactor sites, as well as the presence of ISFSIs located away from any reactor, the staff would seek stakeholder input (as discussed in the Commitments section) on applying existing or developing new definitions (and criteria) for defining the term "site boundary" for ISFSIs.

While the staff would apply the dose limits in Option 2 to both safety and security events, no impacts would be expected for safety events. For security events, certain licensees may have challenges due to the short distance to their controlled area boundary. The options in this paper would provide ISFSI licensees sufficient flexibility to address these challenges. Potential options would include changes to the design of the ISFSI, the use of engineered security features to protect the ISFSI, changes to the ISFSI protective strategy, or changes to the ISFSI emergency planning program (see Enclosure 2 for further discussion of these approaches). Furthermore, this option would not impact the public health and safety objectives currently contained within the ISFSI’s emergency planning program requirements and would continue to support the staff's assumptions that underlie the NRC's 1995 ISFSI emergency planning final rule.

Options 3 and 4 would require reassessment and expansion of the ISFSI emergency planning program requirements, since a foundational assumption from the 1995 ISFSI emergency

planning final rule may no longer be valid (i.e., the dose at the site area boundary could exceed the EPA PAGs' dose limit of 0.01 Sv (1 rem)). Should the Commission conclude that Options 3 or 4 are preferable to Option 2, the staff would need to evaluate several safety, legal, policy, and technical issues, including whether a collocated or a non collocated ISFSI's emergency planning program, capable of classifying events at a "general emergency" level, should contain the same elements as a power reactor's emergency planning program to ensure adequate protection of public health and safety. This would include discussions with the U.S. Federal Emergency Management Agency (FEMA) on whether conforming changes to FEMA's offsite emergency planning regulations would also be necessary.

Issue 3: Should the DBT for radiological sabotage be applied consistently to all ISFSIs (not just to general licensees)?

The majority of ISFSI licensees (30 of the current 45) are general licensees that are already required to establish a physical protection system which protects the spent fuel against the DBT for radiological sabotage in accordance with the power reactor security requirements of 10 CFR 73.55. Changes to the DBT regulations and staff practice have resulted in regulatory questions (uncertainty) on whether a specific-license ISFSI is required to protect the spent nuclear fuel against the DBT for radiological sabotage.

Policy Issue 3 and its options are discussed in more detail in Enclosure 3. The staff has identified three options for Policy Issue 3:

1. Take no action. Do not require specific licensees to protect against the DBT for radiological sabotage. (The regulations would continue to apply the DBT for radiological sabotage to general-license ISFSIs, but not to specific-license ISFSIs.)

2. Continue to apply the DBT for radiological sabotage to general-license ISFSIs. Additionally, apply the DBT for radiological sabotage to specific-license ISFSIs. (The regulations would apply the DBT for radiological sabotage to all ISFSI licensees.)

   (a) Develop a separate adversary characteristics guidance document for ISFSIs; or

   (b) Retain a single adversary characteristics guidance document (applicable to all classes of licensees subject to the DBT for radiological sabotage) and develop an ISFSI-specific sub-tier document.

3. Develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements (ISFSI licensees would not be required to protect the ISFSI against the DBT for radiological sabotage). Develop ISFSI-specific regulatory guidance supporting the new regulations.

The staff recommends Option 3. Both Options 2(a) and 3 would achieve the staff's goals for this rulemaking. Both options are performance-based, both achieve technically acceptable levels of security, and both provide flexibility to ISFSI licensees. However, the staff prefers

Option 3, because: (1) the staff views creation of a risk-informed, performance-based security regulatory structure as providing the greatest support to the Commission's strategic objective of developing performance based regulations by allowing licensees to tailor their security programs and protective measures to the circumstances specific to their ISFSI, while providing the requisite high assurance that the common defense and security will be adequately protected; and (2) the staff does not view the creation of multiple adversary characteristics regulatory guidance documents underlying a singular DBT for radiological sabotage as a vehicle for promoting regulatory clarity.

The staff would use a "risk-informed, performance based" process to define a new regulatory structure for ISFSI security activities. The "risk-informed" element would apply a vulnerability assessment methodology against ISFSIs that is informed by both the intelligence community's developed threat stream and by vulnerability information that is not threat based (i.e., the evaluation of whether ISFSIs may be vulnerable to certain specific weapons effects for which an underlying threat stream does not currently support their inclusion under the DBT for radiological sabotage). The "performance based" element would apply specific radiological dose acceptance limits to ISFSI security activities. This combined approach would provide licensees flexibility in crafting an appropriate security regulatory structure for ISFSIs that may be different than that used for power reactors and would provide clear and objective performance standards. This new approach would recognize that the security regulatory structure applied to ISFSIs may be appropriately different from the security regulatory structure applied to power reactors, due to significant differences in: (1) the designs of these two types of facilities; (2) the nature of their security vulnerabilities; (3) differences in the physical and regulatory approaches used to create defense-in-depth for these facilities; and (4) differences in the nature and size of a potential radiological release from these facilities. The staff envisions an annual review of the threat stream to evaluate whether any changes in the adversary capabilities would differ significantly from the basis for Commission decisions underlying the security assessment frameworks or ISFSI security requirements.

In implementing this option, the staff would develop a regulatory guidance document that describes the details of the ISFSI security-related scenarios in order to support the new regulations. Staff recommendations on the scope and content of this regulatory guidance document (e.g., the use of the power reactor adversary characteristics) are discussed further in Policy Issue 4 (see Enclosure 4). The radiological sabotage scenarios described in the regulatory guidance document would enable ISFSI licensees to perform a CARVER[17] analysis (see Enclosure 5 for background information on CARVER analysis) to determine whether the ISFSI meets the 0.05-Sv (5-rem) dose limit criteria. In recommending this option, the staff additionally recommends continuing the agency's current practice of not performing FOF exercises against ISFSIs.

[17] C.A.R.V.E.R. analysis includes an evaluation against the following factors: Criticality - identify critical assets; Accessability - determine ease of access to critical assets; Recuperability - compare time to repair, replace, or bypass critical assets; Vulnerability - evaluate security system effectiveness against malevolent capabilities; Effect - consider the scope and consequences of the adverse effects from malevolent acts; and Recognizability - evaluate the potential that adversaries would recognize a critical asset.

Regardless of which options the Commission chooses with this policy issue, when combined with the recommendations for Policy Issues 1 and 2 to use a dose-based acceptance criteria, the staff notes that some ISFSIs may be compelled to revise their current protective strategy from a "detect, assess, and communicate" protective strategy to a "denial of task" protective strategy, due to site-specific limitations.

Issue 4: Should the regulatory guidance supporting the performance-based security regulations recommended under Policy Issue 3 be bounded by the (power reactor) adversary characteristics that support the DBT for radiological sabotage?

In Policy Issue 3 the staff recommended development of risk-informed, performance-based security regulations that would apply to all ISFSIs (i.e., both general- and specific-license ISFSIs), in lieu of applying the DBT for radiological sabotage under 10 CFR 73.1. The staff also recommended developing a regulatory guidance document supporting these new regulations that would be specific to ISFSIs. This guidance document would be controlled as Safeguards Information or classified information, as appropriate, and would enable ISFSI licensees to perform an analysis of their facilities as described in Policy Issues 1 and 2.

The regulations currently exempt general-license ISFSIs from some elements of the DBT for radiological sabotage (e.g., the waterborne vehicle bomb assault), thereby setting a precedent for requiring a power reactor licensee with a general-license ISFSI to address different threats which may lead to developing two protective strategies for essentially the same site. Since no specific regulatory guidance supporting the DBT for radiological sabotage has yet been developed for general-license ISFSIs, the staff would need to develop guidance for use by all (general and specific) ISFSI licensees when demonstrating compliance with the performance-based regulations recommended under Policy Issue 3. The current adversary characteristics associated with the DBT for radiological sabotage are focused on power reactors. Therefore, the staff is seeking Commission direction on whether the ISFSI security scenarios should be bounded by the adversary characteristics associated with the DBT for radiological sabotage (as applied to power reactors).

Policy Issue 4 and its options are discussed in more detail in Enclosure 4. The staff has identified three options for Policy Issue 4:

1. Develop ISFSI regulatory guidance that would be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance would be consistent with the power reactor guidance.)

2. Develop ISFSI regulatory guidance that would not be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance document may include capabilities to which ISFSIs may be vulnerable, but to which power reactors are not.)

3. Develop ISFSI regulatory guidance that would be a combination of Options 1 and 2, depending on the location of the ISFSI. ISFSIs located away from any power reactors or ISFSIs collocated with a decommissioning power reactor would follow Option 2. ISFSIs collocated with an operating power reactor would follow Option 1 or Option 2, as follows.

   (a) For collocated ISFSIs (located inside of an operating power reactor's protected area only) the regulatory guidance would be consistent with Option 1. (All other ISFSIs would follow Option 2.); or

   (b) For collocated ISFSIs (located either inside or outside of an operating power reactor's protected area) the regulatory guidance would be consistent with Option 1. (All other ISFSIs would follow Option 2.)

The staff recommends Option 1. This option is consistent with current security requirements for general-license ISFSIs, which are subject to some, but not all, elements of the DBT for radiological sabotage. Overall, this option provides consistent security requirements for protection against radiological sabotage for all ISFSIs, regardless of license type or location. Additionally, this option provides consistency between the scope of the adversary capabilities against which both power-reactor licensees and ISFSI licensees are required to defend.

The staff is recommending this option based principally upon the direction previously provided by the Commission in SRM-SECY-05-0218 on the nature and scope of the adversary characteristics associated with the DBT for radiological sabotage.[18] In contrast, options 2 and 3 would permit ISFSI-specific guidance that is not bounded by the current (operating power reactor) adversary characteristics regulatory guidance (i.e., the suite of adversary characteristics may be different, but would be appropriate for ISFSIs).

However, in recommending Option 1, the staff acknowledges that uncertainty exists on whether additional weapons capabilities may or may not pose a vulnerability to spent fuel storage cask designs. This uncertainty has only been partially assessed by staff, but would involve, for example, adversaries using explosives to create kinetic, shear, or hydrodynamic weapons effects to penetrate a cask's confinement barrier. Because of differences between power reactor critical target sets and ISFSI cask designs, the staff would not expect use of explosives to create these weapons effects, by themselves, to defeat a power reactor target set. The staff acknowledges that an adversary's use of certain types of explosive attacks (using either manufactured or improvised devices)—which the Commission has required certain non-power reactor licensees (but not ISFSIs) to defend against—could likely breach some ISFSI casks' confinement barrier and would thus cause the release of radioactive material. However, the quantity and radionuclide content of the released material and the resultant dose consequences would be significantly influenced by site-specific parameters. Therefore, this type of event may or may not have the potential to yield dose consequences that would exceed a 0.05-Sv (5-rem)

[18] SRM-SECY-05-0218, "Semiannual Threat Environment Review," Classified (ADAMS No. not applicable), dated March 30, 2006.

dose limit at a particular ISFSI's controlled area boundary or exceed a 0.01-Sv (1 rem) dose limit at a particular ISFSI's site area boundary.

Should the Commission conclude that Option 2 or 3 is preferable to Option 1, the staff would recommend assessing additional threat and vulnerability information to support developing the ISFSI-specific regulatory guidance document. Staff would accomplish this assessment in parallel with the development of the technical basis for the proposed rule. Staff would provide the results of the threat and vulnerability evaluation, and any recommendations, to the Commission for its review; and these results and the Commission's review would inform the final technical basis for the proposed rule.

Issue 5: Should the proposed ISFSI security rulemaking apply to future ISFSI licenses only or to both current and future ISFSI licenses?

Given the goals of the proposed ISFSI security rulemaking, the staff has identified two options for Policy Issue 5.

1. The proposed ISFSI security rulemaking would apply to all existing and future ISFSIs.

2. The proposed ISFSI security rulemaking would apply only to ISFSIs licensed subsequent to the effective date of a final rule.

The staff recommends Option 1. Because one of the staff's main goals of this rulemaking is to achieve regulatory consistency for all ISFSIs and to make the security orders generically applicable to all ISFSIs, the staff recommends applying the proposed ISFSI security rulemaking to both current and future ISFSI licenses. Should the Commission chose to apply the proposed ISFSI security rulemaking only to future ISFSIs, the staff would then recommend leaving the ISFSI security orders (on current licensees) in place indefinitely.

The staff views regulatory consistency across a single class of licensees as fundamental regulatory goal for the agency. Applying the rulemaking to the varied types of ISFSI licensees would ensure that the staff could address future, site-specific ISFSI licensing actions in a consistent manner. Additionally, licensees would have sufficient regulatory flexibility to address site-specific issues under the current 10 CFR Parts 72 and 73 exemption processes and under "alternate measures" provisions. The staff would propose using the same "alternate measures" provisions for ISFSI security requirements as were recently approved by the Commission in SRM-SECY-06-0126 for the proposed power reactor security rule (see 10 CFR 73.55(t)).

The principal advantage with Option 2 is that since it would only apply to future ISFSI licensees, no backfit would occur under 10 CFR 72.62. The principal disadvantage is the lack of regulatory consistency.

Issue 6: Should this paper (either in whole or in part) be made available to the public to support the development of the proposed ISFSI security rulemaking?

The staff has not engaged with any external stakeholders in developing this policy paper. Effective communication of these issues, policy options, and proposed solutions during the development of both the technical bases and the proposed ISFSI security rule language will be necessary for a range of stakeholders (e.g., licensees, States, public interest groups, etc.). Consequently, the staff views this Commission paper as an effective vehicle to facilitate stakeholder understanding of these issues and to achieve regulatory transparency and openness in the proposed ISFSI security rulemaking. In considering this issue, the staff was informed by the Commission's direction in SRM-SECY-06-0180[19] to "ensure rulemaking packages reflect potential views of a wider range of stakeholders."

This Commission paper is marked as containing Safeguards Information, consistent with NRC transmittal document requirements; however, when separated from Enclosure 6 it contains only Official Use Only—Security-Related Information. Enclosures 1, 2, 3, and 4, contain Official Use Only—Security-Related Information. Enclosure 5 contains Official Use Only—Sensitive Internal Information. Enclosure 6 contains Safeguards Information and would not be publicly released under any of these options. The staff has identified four options for Policy Issue 6.

1. Do not publicly release this paper or its enclosures.

2. Publicly release this paper only and do not release Enclosures 1 through 5.

3. Publicly release this paper and Enclosures 1 through 5.

4. Publicly release this paper and only redacted portions of Enclosures 1 through 5.

The staff recommends Option 4. Under Option 2 the Commission would approve the decontrol of this Commission paper from Official Use Only—Security-Related Information (OUO-SRI), thus support the public release of a limited amount of information from this paper only. Under Option 3 the Commission would approve the decontrol of both the Commission paper and enclosures 1 through 5, thus supporting the public release of more comprehensive information. Under Option 4, the Commission would approve the decontrol of this Commission paper and staff would redact enclosures 1 through 5 to remove OUO-SRI information, to support their public release. Option 4 would release less information than Option 3, but more information than Option 2. Additionally, under Options 2, 3, or 4 the staff would develop a communications plan to support the release of this information and to obtain stakeholder input for the ISFSI security rulemaking.

[19] SRM-SECY-06-0180, "Supplemental Proposed Rulemaking on Limited Work Authorizations," ADAMS No. ML062750047, dated October 2, 2006.

The staff considers the information in this Commission paper to be of sufficient importance and technical and regulatory complexity to warrant public dissemination to: (1) meet the objectives of SRM-SECY-06-0180; (2) support the development of the technical bases and proposed rule with sufficient publicly-available information for use by non-industry stakeholders; and (3) support the Commission's fundamental goal of regulatory transparency during the rulemaking process. As noted above, no external stakeholders were engaged during the development of this Commission paper. While the staff has prepared this paper at the OUO-SRI level to provide the Commission sufficiently detailed information to facilitate an informed decision, the staff also supports a Commission decision to deliberately decontrol this paper, and portions of the enclosures, to support the agency's ultimate objective of a successful rulemaking.

Because of the complexity of these policy issues and the benefit of communicating detailed information on these issues, the staff views Option 1 as inconsistent with the Commission's previous direction in SRM-SECY-06-0180. The staff views Option 2 as workable, but not preferred, because the degree of regulatory complexity involved in these issues—especially for non-knowledgeable individuals—and the level of detail contained in the enclosures warrants the public release of both the Commission paper and Enclosures 1 through 5, either in whole or in part, to achieve the Commission's goal set forth in SRM-SECY-06-0180. Thus, staff prefers Options 3 and 4 over Option 2. Option 3 publicly releases more sensitive information (the Commission paper and the enclosures), but involves less staff effort (i.e., no redaction of the enclosures is required). Option 4 publicly releases less sensitive information, but requires additional staff effort to appropriately redact the information in Enclosures 1 through 5.

SCHEDULE AND IMPACTS

The staff would begin principal work on the proposed ISFSI security rule in FY 2009. Development of the technical basis for the rulemaking would be completed by the end of FY 2008, subsequent to the receipt of Commission direction on this paper. The staff is not proposing to submit a rulemaking plan for this rulemaking, since this policy paper addresses the substantive issues associated with the proposed rulemaking.

The staff estimates the resources required to accomplish the staff reviews of licensee assessments recommended under Policy Issue 1 would involve 1.5 staff-months to review each ISFSI's analysis to verify compliance with the 0.05-Sv (5-rem) dose limit criterion. Currently, there are 45 licensed ISFSIs that would need to be evaluated requiring an estimated 5.6 FTE and $225K spread out over a 3-year period. The staff would anticipate beginning such reviews in FY 2011 (i.e., approximately a year after the issuance of a final rule—which the staff anticipates would be by the end of FY 2010). Resources for staff reviews of these current ISFSIs and any future ISFSI license applications would be addressed in out-year budgets via the agency’s planning, budgeting, and performance management (PBPM) process.

As an aid to the Commission's deliberations and recognizing that industry has not been approached on these rough cost numbers, the staff is providing the following estimates of numbers of impacted licensees and of potential licensee expenses to implement the policy options recommended in this paper. Licensee accomplishment of the recommended

assessments would likely require a multi-discipline team with engineering, health physics, and security expertise. Given these caveats, the staff would estimate (out of the current population of 45 ISFSIs) that (1) 40 ISFSIs would require 0.5 to 1 staff months ($20K to $41K) to verify their ISFSI meets the proposed dose limits without significant additional effort; (2) 4 ISFSIs would require 1 to 2 staff months ($41K to $82K) to perform more detailed or iterated calculations to verify their ISFSI meets the proposed dose limits; and (3) 1 ISFSI would require an additional 6 staff months (i.e., 7 to 8 months total) ($289K to $330K) to revise their security plan or emergency plan to meet the dose limits. The staff used a rate of $258 per hour from the FY 2007 fee rule in making these estimates. Alternatively, if instead changes to its security plan or emergency plan, the ISFSI licensee in (3) above had to make changes to the design of its ISFSI, move its ISFSI, use engineered security features to provide additional security, or purchase additional land to meet the dose limits, then costs of such changes could range from $750K to $7.5M or more depending on the specific site and the nature of the changes.

COMMITMENTS:

The staff will accomplish the proposed ISFSI security rulemaking as previously directed by the Commission.

If the Commission approves the staff's recommendation for Policy Issue 6 (i.e., Option 4), the staff will develop a communication plan to: (1) support the public release of this paper and any redacted enclosures; and (2) engage stakeholders during development of the technical basis and the proposed ISFSI security rulemaking.

RECOMMENDATIONS:

The staff recommends that the Commission approve the following policy options:

Issue 1: Should a radiological acceptance criterion be applied consistently to all ISFSIs?

The staff recommends Option 4(b): *Apply the radiological dose criterion to all ISFSIs. The licensee performs the assessments and demonstrates the ISFSI is in compliance with the dose limit*.

Issue 2: Should the dose limits for acts of radiological sabotage (if any are established under Policy Issue 1) be the same as the dose limits for safety-related DBAs?

The staff recommends Option 2: *Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary); and also meet a 0.01-Sv (1-rem) dose limit for both safety and security events at the site area boundary.*

Issue 3: Should the DBT for Radiological Sabotage Be Applied Consistently to All ISFSIs (Not Just to General Licensees)?

The staff recommends Option 3: *Develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements (ISFSI licensees would not be required to protect the ISFSI against the DBT for radiological sabotage). Develop ISFSI-specific regulatory guidance supporting the new regulations.*

Issue 4: Should the regulatory guidance supporting the performance-based security regulations recommended under Policy Issue 3 be bounded by the (power reactor) adversary characteristics that support the DBT for radiological sabotage?

The staff recommends Option 1: *Develop ISFSI regulatory guidance that would be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance would be consistent with the power reactor guidance.)*

Issue 5: Should the proposed ISFSI security rulemaking apply to future ISFSI licensees only or to both current and future ISFSI licensees?

The staff recommends Option 1: *The proposed ISFSI security rulemaking would apply to all existing and future ISFSI licenses.*

Issue 6: Should this paper (either in whole or in part) be made available to the public to support the development of the proposed ISFSI security rulemaking?

The staff recommends Option 4: *Publicly release this paper and only redacted portions of Enclosures 1 through 5.*

RESOURCES:

The resources required to accomplish the development of the technical basis and the proposed ISFSI security rulemaking implementing the recommendations of Policy Issues 1, 2, 3, 4, and 6 are as follows:

(1) The Office of Nuclear Security and Incident Response (NSIR) estimates these resources to be 0.3 FTE in FY 2007, 0.3 FTE in FY 2008, 0.7 FTE and $100K in FY 2009, and 0.7 FTE in FY 2010.

(2) The Office of Federal and State Materials and Environmental Management Programs (FSME) estimates these resources to be 0.8 FTE in FY 2009 and 0.7 FTE in FY 2010.
(3) The Office of Nuclear Material Safety and Safeguards (NMSS) estimates these resources to be 0.3 FTE in FY 2008.

These resources are currently budgeted for FY 2007 and FY 2008. Resources for FY 2009 are included in the proposed budget that was submitted to the Commission. Resources for FY 2010 would be addressed via the agency's PBPM process.

The resources required to develop the supporting regulatory guidance for the proposed ISFSI security rulemaking under Policy Issue 4 is 0.2 FTE in FY 2008 for NSIR. This resource is budgeted. However, if the Commission concludes further analysis is required of potential ISFSI vulnerabilities (to address certain uses of explosives) not previously analyzed, NSIR would need an additional 0.2 FTE in FY 2007 and 0.2 FTE in FY 2008. Those resources are currently unbudgeted.

The resources required to accomplish the recommendation for Policy Issue 6 and associated communications plan are 0.1 FTE in FY 2007 for NSIR. NMSS resources for the communication plan are included in the 0.3 FTE in FY 2008 mentioned above in item (3). These resources are currently budgeted in NSIR and unbudgeted in NMSS. The information on resources and schedules reflect the current planning environment. If a significant amount of time (greater than 90 days) passes, or the Commission provides the staff direction that differs from or adds to the staff's recommended actions, this section and the schedule and impacts section of the paper would need to be revisited after issuance of the draft SRM.

COORDINATION:

The Office of the Chief Financial Officer has reviewed this Commission Paper for resource implications and has no objection. The Office of the General Counsel has reviewed this Commission Paper and has no legal objection.

/RA/

Luis A. Reyes
Executive Director
for Operations

Enclosures:
1. Policy Issue 1 Analysis **(Redacted)**
2. Policy Issue 2 Analysis **(Redacted)**
3. Policy Issue 3 Analysis **(Redacted)**
4. Policy Issue 4 Analysis **(Redacted)**
5. Background Information on Threat Assessments and CARVER Analysis **(Redacted)**
6. Response to ISFSI Security Questions (contains Safeguards Information)

Should a Radiological Acceptance Criterion for Security Scenarios Be Applied Consistently To All ISFSIs? (Policy Issue 1)

Summary

Specific-license independent spent fuel storage installations (ISFSIs) are currently required under 10 CFR 73.51, “Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-level Radioactive Waste,” to meet a 0.05-Sv (5-rem) dose limit for acts of radiological sabotage.[1] The regulations do not currently specify an explicit dose limit for security events for general-license ISFSIs. The staff has historically considered general licensees—which are required under 10 CFR 72.212, "Conditions of general license issued under § 72.210," to protect the spent fuel against the design basis threat (DBT) for radiological sabotage—as having the same level of protection required of specific licensees (i.e., all ISFSIs are protected to the same level). The staff has identified four options to consistently apply or not apply a dose limit for security events for all ISFSIs:

1. Retain the current dose limits and clarify the applicability of the ISFSI security requirements.

2. Eliminate the radiological dose criterion for all ISFSIs and apply the current protective strategy, which includes the security orders.

3. Eliminate the radiological dose criterion for all ISFSIs and require ISFSI licensees to prevent or impede attempted acts of radiological sabotage.

4. Apply the radiological dose criterion to all ISFSIs.

    (a) The staff performs the assessments to determine whether the ISFSI is in compliance with the dose limit; or

    (b) The licensee performs the assessments and demonstrates that the ISFSI is in compliance with the dose limit.

The staff recommends Option 4(b). This option is performance-based, and affords the ISFSI licensee the greatest amount of flexibility in meeting the regulations. This option is also consistent with the historic NRC regulatory model requiring licensees to demonstrate compliance, and minimizes licensee fee costs and the impact on staff resources. Additionally, this option provides consistency for the differing types of ISFSI licensees, and also provides a metric that is independent of future fuel loading characteristics and dry-cask storage designs.

[1] Currently, the dose criteria in Title 10 of the *Code of Federal Regulations* (CFR) 72.106, "Controlled Area of an ISFSI or MRS," are 0.05 Sievert (Sv) (5 rem) total effective dose equivalent; 0.15 Sv (15 rem) to the lens of the eye; or 0.5 Sv (50 rem) as either the sum of the deep dose equivalent and any organ dose, or the shallow dose equivalent to the skin or any extremity. For simplicity, these limits are hereinafter referred to as the 0.05-Sv (5-rem) dose limit.

The licensee's assessments that their ISFSI was in compliance with the dose limits would be subject to review and/or inspection by the staff, as appropriate.

Under a dose-based acceptance criteria, some ISFSI licensees might have to revise their current protective strategy from a "detect, assess, and communicate" protective strategy to a "denial of task" protective strategy due to site-specific limitations (e.g., limited room to expand the distance between their ISFSI and their controlled area boundary). Consequently, if a constrained licensee cannot meet the dose limit through the use of passive security measures (e.g., the use of engineered security features or through changes to the ISFSI's design), one of the options available to the licensee would be to use active security measures (e.g., a "denial" protective strategy) to prevent a successful terrorist attack. However, the staff envisions that only very few licensees may be sufficiently constrained to be unable to meet the radiological dose criterion through the use of passive security measures and thus would be compelled to shift to a "denial of task" protective strategy.

<u>Background</u>

Section 73.51 currently requires specific-license ISFSIs to meet a 0.05-Sv (5-rem) dose limit for security events. The regulations do not currently specify an explicit dose limit for security events for general-license ISFSIs. The staff's historical perspective was that general-license ISFSIs, which are required to protect against the DBT for radiological sabotage, have the same level of protection as is required for specific-license ISFSIs.

Although the regulations do not require general-license ISFSIs to meet a 0.05-Sv (5-rem) dose limit for security events, since [redacted] the staff's practice has been to ensure that general-license ISFSIs, as well as specific-license ISFSIs, meet this criterion. [redacted].

[redacted]. Every ISFSI licensee [redacted] was informally requested by staff to use a minimum distance to their controlled area

boundary [redacted]. Every licensee acceded to the staff's informal request. The staff did not revisit the issue of a minimum [redacted] distance to the controlled area boundary [redacted], largely because efforts to do so were interrupted by the events of September 11, 2001. Consequently, the 0.05-Sv (5-rem) dose limit has been effectively applied to all ISFSI licensees [redacted], including general licensees, by the staff informally requesting a minimum distance [redacted] to the controlled area boundary. However, no ISFSI licensee has been required to verify compliance with a 0.05-Sv (5-rem) dose limit.

Before [redacted], the staff believed that the consequences of security scenarios were bounded by the consequences resulting from (safety-related) design-basis accidents (DBAs), such that licensees meeting the 0.05-Sv (5-rem) dose limit for safety-related events, would also meet a 0.05-Sv (5-rem) dose limit for any security-related events invoked by 10 CFR 73.51(b)(3). [redacted] the staff determined that licensees would comply with 10 CFR 73.51(b)(3) as long as their distance to the controlled area boundary was at least [redacted]. [redacted] the staff's informal practice was to apply a minimum distance [redacted] to the controlled area boundary for any new ISFSI licensee, thereby obviating the need for the licensee to verify compliance with a dose limit.

Discussion

Based upon [redacted] in SECY-06-0045,[2] the staff has gained new insights indicating that a minimum distance [redacted] to the controlled area boundary may no longer be bounding for all ISFSI licensees. The events of September 11, 2001, caused the staff to reevaluate both the threat environment and the previously studied scenarios. [redacted] under SECY-06-0045 have shown that the staff should not necessarily rely [redacted] to ensure that all ISFSI licensees meet the 0.05-Sv (5-rem) dose limit for security events.

As discussed in Enclosure 6 to this paper,[3] the SECY-06-0045 security assessments were generic for different storage cask types (i.e., the same threats, meteorological conditions, and spent fuel characteristics were applied to each storage cask design in order to evaluate the consequences from the major cask designs currently in use). However, the resulting offsite dose from an ISFSI sabotage event depends on factors that would likely vary between sites, including: (a) the spent fuel characteristics (assembly design, burnup, and cooling time); (b) the spent fuel storage cask design and fuel loading; and (c) the site characteristics (the distance

---

[2] SECY-06-0045, "Results of Implementation of the Decisionmaking Framework for Materials and Research and Test Reactor Security Assessments," ADAMS No. ML060340452, dated March 1, 2006. **[Non-public]**

[3] Enclosure 6, "Response to ISFSI Security Questions." **[Non-public]**

from the nearest cask to the controlled area boundary, meteorological conditions, topography, etc.). Based on the results from the staff's security assessment and the evaluations performed for the sites discussed in Enclosure 6, it is likely that most ISFSIs currently meet the dose requirements for security events—largely because these ISFSIs are currently loading and storing their older, colder spent fuel and also because they have distances from the ISFSI to the controlled area boundary that exceed the regulatory minimum of 100 meters (328 feet). However, if ISFSI licensees ■■■■■■■■■■■■■■■■ loading high burnup and/or hotter fuel into storage casks, (which is permitted under many cask designs), the security assessment calculations indicate that for security events some ISFSIs may no longer meet the 0.05-Sv (5-rem) dose limit at their current controlled area boundary.

Licensee Submittal of Security Plans for NRC Prior Review and Approval

No ISFSI licensees currently implement a "denial of task" protective strategy. However, under a dose-based acceptance criteria, some ISFSI licensees might have to revise their current protective strategy from a "detect, assess, and communicate" protective strategy to a "denial of task" protective strategy due to site-specific limitations (e.g., limited room to expand the distance between their ISFSI and their controlled area boundary). Consequently, if a constrained licensee cannot meet the dose limit through the use of passive security measures (e.g., the use of engineered security features or through changes to the ISFSI's design), one of the options available to the licensee would be to use active security measures (e.g., a "denial of task" protective strategy) to prevent a successful terrorist attack. The staff envisions that only very few licensees may be sufficiently constrained to be unable to meet the radiological dose criterion through the use of passive security measures and thus would be compelled to shift to a "denial of task" protective strategy.

The use of a "denial of task" protective strategy raises issues of sufficient technical complexity to necessitate prior staff review and approval of a licensee's security plan. The staff bases this conclusion on (1) experience gained in the CY 2003 - CY 2004 reviews of changes to reactor security plans to implement the security and DBT orders and the resultant degree of complexity and the need for interactions with licensees, and (2) a desire to maintain an appropriate independence and separation of security plan review and inspection functions. For a specific-license ISFSI, NRC prior review and approval of applicant's initial security plans is required under the current regulations.[4] Under 10 CFR 72.44(e), ("License conditions"), a specific-license ISFSI may make certain changes to their security plan without NRC prior review and approval, if such changes do not decrease the effectiveness of the security plan. For a general-license ISFSI, the security requirements for the ISFSI are incorporated in the security plan (required under Part 50) for the associated power reactor license and are subject to inspection by NRC regional staff, not to staff prior review and approval. Similarly, reactor

[4] 10 CFR 72.40(a)(8), "Issuance of license," requires a staff finding that an applicant's physical security program (i.e., security plan) for a specific-license ISFSI complies with the security requirements of Subpart H of Part 72. See Figure 1 for a discussion of how the current security regulations apply to a specific-license ISFSI.
10 CFR 72.24(o), "Content of application: Technical information," requires applicants for a specific license to submit their security plans to the NRC (as part of their license application) for prior review and approval.

licensees are permitted under 10 CFR 50.54(p)(1), ("Conditions of licenses"), to make certain changes to their security plan without prior NRC review and approval, provided such changes do not decrease the effectiveness of their security plan. In all likelihood, a general-license ISFSI's shift to a denial protective strategy would not decrease the effectiveness of the associated power reactor's security plan under 10 CFR 50.54(p)(1). However, as discussed earlier in this paragraph and notwithstanding the provisions of 10 CFR 50.54(p)(1), the staff would revise the regulations to require a reactor licensee, associated with a general-license ISFSI who chooses to employ a "denial of task" protective strategy for the ISFSI, to submit its security plan (for protecting both the reactor and ISFSI) to the NRC for prior review and approval. The NRC's approval of a revised security plan for the site would be a specific licensing action under the Part 50 license that would create a potential hearing right.[5]

However, the staff notes that some Part 50 licensees who are currently using the Part 72 general license process have required amendments to their Part 50 license to accommodate the presence of the ISFSI, thus creating a potential hearing right under the Part 50 license. An example of this was for heavy loads issues (e.g., the use of single failure proof cranes and revised heavy load pathways). Therefore, revising the necessary regulations to require a general-license ISFSI, who was compelled to adopt a "denial of task" protective strategy, to submit the site (reactor and ISFSI) security plan to the NRC for review and approval would be consistent with the current Part 50 reactor license/Part 72 general-license ISFSI regulations. Consequently, the staff's view is that the potential for hearing requests would be essentially the same as it is under the current regulations. Furthermore, as noted above, the staff expects that very few licensees would be sufficiently constrained by site-specific limitations to be unable to retain their current "detect, assess, and communicate" protective strategy, and thus would be compelled to shift to a "denial of task" protective strategy.

Separately, the staff notes that if an ISFSI licensee were to apply to the NRC to use enhanced weapons (e.g., machineguns) to protect their ISFSI, as provided under new section 161A of the AEA,[6] that licensee would also be required to submit their security plans to the NRC for prior review and approval. This would be a new requirement for any ISFSIs applying to use enhanced weapons. Prior review and approval of security plans using enhanced weapons is a component of the ■■■■■■■■■■■■■■■■■■■■■■■■■■■■ firearms guidelines and implementing language for this provision (for power reactors only) was provided in the recently published proposed power reactor security rule.[7]

---

[5] The current Part 72 general license regulations implement provisions of Section 218(a) of the Nuclear Waste Policy Act of 1982, as amended (42 U.S.C. 10198), that mandated that the Commission by rule approve technologies for the dry storage of spent fuel at civilian nuclear power reactors, "without to the extent practicable," the need for additional site specific [licensing] approvals by the Commission. Under the current Part 72 general license regulations, no site-specific licensing actions are required to use dry storage casks to store spent fuel.

[6] Section 161A was added to the AEA under Section 653 of the EPAct (42 U.S.C. 2201a).

[7] SECY-06-0126, "Proposed Rulemaking - Power Reactor Security Requirements," ADAMS No. ML00830634, dated May 31, 2006. Published for comment in the *Federal Register* (72 FR 62663) on October 26, 2006.

The staff further notes that it is not proposing a requirement to convert general-license ISFSIs to specific-license ISFSIs, were the licensee required to implement a “denial of task” protective strategy. Instead, as discussed above, the staff would propose requiring a Part 50 licensee, who is constrained to adopt a "denial of task" protective strategy for its Part 72 general-license ISFSI, to submit a modified site security plan (that encompasses both the reactor and ISFSI) to the NRC for prior review and approval, notwithstanding the provisions of 10 CFR 50.54(p)(1).

Issue 1 Options

1. *Retain the current dose limits and clarify the applicability of the ISFSI security requirements.*

   This option requires the already-planned actions to make the ISFSI security orders generically applicable and to clarify the applicability of the Part 73 regulations to both general and specific licensees. Non-collocated, specific licensees would be the only ISFSI licensees required to meet the 0.05-Sv (5-rem) dose limit criterion for security events. The remaining majority of ISFSI licensees (those located at reactors with operating licenses) would not. All ISFSI licensees would have to continue to conform with the prescriptive requirements in the ISFSI security orders that would be made generically applicable during the rulemaking.

   Although this option only requires clarifying changes to the regulations, it would require a departure from past practice for either the licensees or the staff. As discussed above, the staff has not previously required non-collocated, specific licensees to demonstrate compliance with the 0.05-Sv (5-rem) dose limit for security-related events. However, as discussed above, ■■ may no longer be bounding for every ISFSI site (i.e., ■■■■■■■■■■■■■■■■■■■■■■■■ minimum distance to the controlled area boundary may not ensure that all licensees meet the 0.05-Sv (5-rem) dose limit). Therefore, this option would require either the non-collocated, specific licensees or the staff to perform dose calculations to determine whether the licensee complies with the 0.05-Sv (5-rem) dose limit for security scenarios.

   If the staff performs the dose assessments for the few licensees (there are only seven non-collocated, specific ISFSIs) that are required to meet the 0.05-Sv (5-rem) dose limit, there would be no added burden on the licensees to perform dose assessments. Additionally, if the staff performs the dose assessments, this option has the advantage of limiting the dissemination of sensitive and/or classified information that is necessary to perform the calculations. However, the licensees may not have the same degree of flexibility in developing solutions to meet the regulations as they would if they were performing the calculations themselves. For example, if a licensee were assessing various means to ensure compliance, then the licensee may find a more efficient and less costly means of meeting the regulations other than by increasing the distance to

their controlled area boundary. The staff may not recognize all the options available to the individual sites when performing the consequence assessments and recommending changes to the physical protection plans. Alternatively, the results of the staff's analysis may cause the licensee to consider different approaches for its physical protection plan or protective strategy. Such changes would then require the staff to reperform the consequence assessment. This process could be repeated several times as the licensee evaluates potential options, since the licensee would not have all the information developed during the staff evaluations.

If the staff were to start requiring site-specific ISFSI licensees to demonstrate compliance with the 0.05-Sv (5-rem) dose limit for security scenarios, the non-collocated, specific licensee would have to perform calculations that they were not previously required to perform. If the licensees perform the calculations, the staff would need to share sensitive and/or classified information such that the licensees would know which security scenarios to evaluate in order to demonstrate compliance with the dose limit. Because not all ISFSI licensees would be required to meet a dose limit, this would result in some, but not all, licensees having access to sensitive or classified information. Additionally, the staff would likely need to issue some regulatory guidance on an acceptable methodology for performing the dose assessments and would also need to review and/or inspect the licensee's evaluations.

This option has a few advantages. Under this option, the staff would not have to develop a technical basis for requiring the currently exempt licensees to meet 10 CFR 73.51(b)(3). Additionally, this option would not set a precedent for other licensees or licensed activities that currently do not have a dose limit for security scenarios, such as spent fuel transportation and sealed-source manufacturers and distributors.

However, this option has several disadvantages. Site-specific ISFSI licensees at power reactor sites that undergo decommissioning (i.e., shift from an operating to a possession-only license status) would not have consistent security requirements. Specifically, when the reactor holds a license to operate, the ISFSI is not required to meet a dose limit for security scenarios; but when the reactor licensee switches to a possession-only license, the ISFSI would then be required to meet a 0.05-Sv (5-rem) dose limit for specified security scenarios. An ISFSI in this situation (i.e., transferring from a collocated, specific licensee to a non-collocated, specific licensee) would have to evaluate whether the 0.05-Sv (5-rem) criterion is met before the reactor licensee switches from the operating to possession-only license and would likely have to supplement its physical protection plan.

Another disadvantage to this option is the continued lack of consistent security requirements for the different types of ISFSI licensees. Some future ISFSI sites may load combinations of fuel into casks that are not bounded by current analyses, and no radiological criterion would be in place to limit the potential dose resulting from a terrorist

attack. For example, loading high-burnup fuel, loading fuel with shorter cooling times, or loading into new, as-of-now-unlicensed cask designs, are all factors that may increase the radiological consequences resulting from a terrorist attack, even if the threat environment remains unchanged.

General-license ISFSIs are exempted, via 10 CFR 72.212(b)(5)(v), from the requirements of the current 10 CFR 73.55(h)(4)(iii)(A), ("Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage"), which requires licensees to "… prevent or impede attempted acts of radiological sabotage …." Therefore, the current protective strategy for a general-license ISFSI does not require the licensee to prevent or impede attempted terrorist attacks from succeeding, but instead relies upon local law enforcement personnel to neutralize the adversaries after detection and assessment by the licensee. Additionally, specific-license ISFSIs subject to 10 CFR 73.51 are not required to design their physical protection systems to defend against the DBT for radiological sabotage, but are required to provide high assurance that the storage of spent fuel does not constitute an unreasonable risk, i.e., one that would exceed a 0.05-Sv (5-rem) dose limit. Accordingly, the staff's view is that establishment of a radiological criterion for security scenarios, will provide greater certainty that public health and safety is being protected with high assurance from malevolent attacks.

2. *Eliminate the radiological dose criterion for all ISFSIs and apply the current protective strategy, which includes the security orders.*

This option would require all ISFSI licensees to meet the same regulations. Although ISFSI licensees would still be required to meet the 0.05-Sv (5-rem) dose limit for (safety-related) DBAs the radiological criterion would be eliminated for specified security scenarios. All ISFSI licensees would have to continue to conform with the prescriptive requirements in the ISFSI security orders that would be made generically applicable in the proposed ISFSI security rulemaking.

This option has a few advantages. Under this option, there would be no added burden on the staff or the licensee to perform dose assessments, and this option has the advantage of limiting the dissemination of sensitive and/or classified information. This option also provides consistency in security requirements for all ISFSI licensees. Additionally, this option would not set a precedent for other licensees or licensed activities which currently do not have a dose limit for security scenarios, such as spent-fuel transportation and sealed-source manufacturers and distributors.

However, this option has several disadvantages. It would appear to reduce the security requirements for non-collocated, specific licensees, which could negatively impact public confidence. Additionally, this option may not be consistent with assumptions used in site-specific environmental impact statements (e.g., the assumption that a dose at the controlled area boundary resulting from a security scenario would not exceed a 0.05-Sv

(5-rem) dose limit), and likely would result in significant licensee and staff effort in revisiting and updating the current environmental evaluation. Removing the dose limit for specified security scenarios may also affect emergency planning requirements such that non-collocated, specific ISFSIs may have to develop more comprehensive emergency plans. (See Policy Issue 2 for a fuller discussion of ISFSI emergency planning versus dose issues.)[8]

Another disadvantage associated with this option is that, as discussed in more detail under Option 1, some future ISFSI sites may load combinations of fuel into casks that are not bounded by current analyses, and no radiological criterion would be in place to limit the potential dose resulting from a terrorist attack. Essentially, if this option were adopted, the Commission would need to rely on the prescriptive security measures imposed on the licensees to ensure adequate protection of public health and safety. Significant staff effort would be required to evaluate the technical bases supporting the rulemaking to ensure that the prescriptive security measures are sufficient (without a dose limit requirement) to limit the potential consequences of a security-related event.

3. *Eliminate the radiological dose criterion for all ISFSIs and require ISFSI licensees to prevent or impede attempted acts of radiological sabotage.*

This option would require all ISFSI licensees to meet the same regulations. Although ISFSI licensees would still be required to meet the 0.05-Sv (5-rem) dose limit for (safety-related) DBAs, the radiological criterion would be eliminated for specified security scenarios. All ISFSI licensees would have to continue to conform with the prescriptive requirements in the ISFSI security orders. Furthermore, ISFSI licensees would have to prevent or impede attempted acts of radiological sabotage, such that a release of radioactive material would not occur. For example, use of a below ground ISFSI would "prevent" certain acts of radiological sabotage from succeeding

This option has a few advantages. It would provide assurance that ISFSI licensees would adequately protect the public from terrorist attacks, and would also provide a consistent protective strategy for all ISFSI licensees. Additionally, this option ensures consistency between both ISFSI- and reactor-protective strategies. Because ISFSI licensees would not be required to perform dose assessments, this option limits the need to disseminate sensitive and/or classified information to a broader group of licensees and/or cask certificate holders (i.e., cask vendors).

However, this option has several disadvantages. Perhaps the greatest disadvantage is the backfit and significant cost burden placed on ISFSI licensees to upgrade their protective strategies so that they are able to prevent or impede attempted acts of radiological sabotage (i.e., implementing a "denial of task" protective strategy). This

[8] Enclosure 2, "Should the Dose Limits for Acts of Radiological Sabotage (If Any Are Established under Policy Issue 1) Be the Same as the Dose Limits for Design-basis Accidents?"

option represents a significant departure from previous Commission requirements for ISFSI licensees. Additionally, this option may be precedent-setting for other non-reactor facilities and/or activities, such as spent fuel transportation (i.e., there are currently no regulations requiring transporters of spent fuel to impede terrorist attacks). The public may have a difficult time understanding the Commission's rationale on why such drastically different protective strategies are placed on spent nuclear fuel in dry storage casks, but not on spent nuclear fuel in transportation packages, which in some cases is the same identical physical storage cask/transportation package. Finally, this option would require the staff to dedicate a significant amount of resources toward developing the technical basis for increasing the ISFSI protective strategy.

4. *Apply the radiological dose criterion to all ISFSIs.*

   (a) Staff performs the assessments to determine whether the ISFSI is in compliance with the dose limit.

This option keeps the current protective strategy, and includes making the ISFSI security orders generically applicable. Under this option, all ISFSI licensees would be required to meet the same regulations. ISFSI licensees would be required to meet the 0.05-Sv (5-rem) dose limit for (safety-related) DBAs, as well as for specified security scenarios; however, the staff would perform the assessments to ensure compliance with the dose limit. All ISFSI licensees would have to continue to conform with the prescriptive requirements in the ISFSI security orders, which would be made generically applicable to all ISFSI licensees.

This option has several advantages. Perhaps the greatest advantage is that, by bringing consistency to the regulations, the Commission would have assurance that all ISFSI licensees would be protecting to the same level, regardless of ISFSI license type and location. This option does not need to assume that defending against the DBT provides the same level of protection as a 0.05-Sv (5-rem) dose limit for security scenarios, since the dose limit would be applied to all ISFSI licensees.

This option also has the advantage of not directly burdening the licensees to perform the dose consequence assessments. However, the staff would have perform the dose consequence assessments as a fee-based activity. The staff would then work with the individual licensees to ensure that their protective strategy adequately ensures that no release with a potential for exceeding the dose limit would occur as a result of the postulated terrorist attack. Since the licensees would not need security scenario and/or threat information to perform calculations, this option limits the dissemination of such sensitive and/or classified information.

However, this option also has several disadvantages. Even though this option is performance-based, the staff is performing the dose assessments to determine whether the licensee is in compliance. Consequently, licensees may not have the same amount

of flexibility or understanding of the potential options in meeting the regulations as if they performed the analysis themselves. For example, if a licensee were performing the dose calculation to determine compliance, the licensee may find a more efficient and less costly means of meeting the regulations other than by increasing the distance to their controlled area boundary. The staff may not recognize all the options available to the individual sites when performing the consequence assessments. Alternatively, a license (because of limitations specific to its site) may be compelled to implement a "denial of task" protective strategy. Furthermore, the results of staff's analysis may cause the licensee to consider different approaches for its physical protection plan or protective strategy, which would then require the staff to reperform the consequence assessment (all of which would be subject to additional fees). This process could be repeated several times as the licensee evaluates potential options, since the licensee would not have all the information developed during the staff's assessment.

Additionally, this option is also disadvantageous because it requires the staff, rather than the ISFSI licensee, to demonstrate compliance with the regulations. Thus, this option would require significant staff effort. As discussed earlier in this enclosure, the staff has demonstrated compliance for ISFSI licensees in the past, because of exigent circumstances (i.e., information security concerns). However, this approach was a departure from the historic NRC regulatory model in which the licensee is responsible for demonstrating compliance with the regulations and the staff is responsible for verifying that the licensee's demonstration of compliance is adequate. Fundamentally, the staff's view is that the burden of proof for meeting the regulations ultimately rests on the licensee.

Finally, this option would likely impose a backfit on those ISFSI licensees that are not currently specifically required to meet a radiological criterion for security scenarios.

(b) Licensee performs the assessments and demonstrates that the ISFSI is in compliance with the dose limit.

This option would require all ISFSI licensees to meet the same regulations. ISFSI licensees would be required to demonstrate compliance with the 0.05-Sv (5-rem) dose limit for (safety-related) DBAs, as well as for specified security scenarios. All ISFSI licensees would have to continue to conform with the prescriptive requirements in the orders, which would be made generically applicable to all ISFSI licensees.

This option has several advantages. As in Option 4(a) above, the greatest advantage would be that, by bringing consistency to the regulations, the Commission would have assurance that all ISFSI licensees would be protected to the same level, regardless of license type and location. This option does not need to assume that defending against the DBT for radiological sabotage provides the same level of protection as a 0.05-Sv (5-rem) dose limit for security scenarios.

This option has the added advantage of placing the responsibility for demonstrating compliance on the ISFSI licensees, rather than on the staff. This approach would be consistent with the historic NRC regulatory model of the licensee demonstrating compliance, and it has the further advantage of providing flexibility to the licensee in meeting the regulations. A licensee would be able to assess how to best meet the dose limit at its site (e.g., through limiting the spent fuel characteristics, extending the distance to the controlled area boundary, etc.). Additionally, the staff would expend much fewer resources because the staff would not have to perform multiple analyses per site, if the licensees choose to evaluate various protective strategy options.

Despite its advantages, this option is not without its disadvantages. As with Option 4(a), use of dose-based limits could compel licensee with limitations specific to their site to adopt a "denial of task" protective strategy. Additionally, because the burden would be on the licensees to accomplish the assessments, the staff would be required to provide licensees with the necessary Safeguards Information and/or classified information to perform the assessments. Therefore, the staff would have to establish controls to limit the dissemination of sensitive and/or classified information pertaining to the specified security scenarios. Additionally, the staff recognizes that some licensees may turn to contractors (e.g., the cask certificate holder (i.e., vendor)) to perform these consequence analyses, thus broadening the potential range of dissemination of this information. It is likely, however, that the staff could develop sufficient guidance at the Safeguards Information level for the licensees' dose assessment calculations. As in safety reviews, the staff may receive a wide variety of methodologies for demonstrating compliance, which may complicate and/or lengthen staff reviews.

Finally, similar to Option 4(a), this option would likely impose a backfit on those ISFSI licensees that are currently not specifically required to meet a radiological criterion for security scenarios.

Issue 1 Recommendation

The staff recommends Option 4(b), "Apply the radiological dose criterion to all ISFSIs. The licensee performs the assessments and demonstrates that the ISFSI is in compliance with the dose limit." This option is performance-based, and affords the ISFSI licensee the greatest amount of flexibility in meeting the regulations. This option is consistent with the historic NRC regulatory model requiring licensees to demonstrate compliance, and minimizes licensee fee costs and the impact on staff resources. Additionally, this option provides consistency for the differing types of ISFSI licensees, and also provides a metric that is independent of future fuel loading characteristics and dry-cask storage designs. The licensee's assessments would be subject to review and/or inspection by the staff, as appropriate.

The staff notes that for all options discussed above—which all have a dose-based acceptance criteria—some ISFSIs might have to revise their current protective strategy from a "detect, assess, and communicate" protective strategy to a "denial of task" protective strategy. The

reason for this change is that some licensees (due to limitations at their specific site, e.g., the inability to expand the distance between the ISFSI and the controlled area boundary) may be constrained in their options to meet the radiological dose criterion; and thus may be compelled to shift to a "denial of task" protective strategy. The staff would propose requiring ISFSI licensees that choose to use of a "denial of task" protective strategy to provide their applicable security plans to the NRC for prior review and approval.

Should the dose limits for acts of radiological sabotage (if any are established under Policy Issue 1) be the same as the dose limits for design-basis accidents? (Policy Issue 2)

Summary

In the current regulations, the dose limit for security scenarios for non-collocated, specific-license independent spent fuel storage installations (ISFSIs) is consistent with the design-basis accidents (DBAs) (i.e., 0.05-Sv (5-rem) dose limit).[1] As discussed in the statements of consideration accompanying the final rule promulgating the initial regulations for 10 CFR Part 72,[2] this dose limit was derived from protective actions recommended by the U.S. Environmental Protection Agency (EPA) for projected doses to populations for planning purposes. Additionally, under a 1995 ISFSI emergency planning final rule the Commission concluded that a release exceeding the EPA Protective Action Guidelines (PAGs) would not occur;[3] consequently, no verification was required that doses would be less than 0.01 Sv (1 rem) at the site area boundary. If the Commission determines, under Policy Issue 1 (see Enclosure 1 to this paper),[4] that a radiological acceptance criterion for acts of radiological sabotage should be applied to all ISFSI licensees, is a 0.05-Sv (5-rem) dose limit criteria still the appropriate limit? The staff has identified four options for Policy Issue 2:

1. Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary).

2. Keep the dose limit for radiological sabotage consistent with the dose limit for DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary); and also meet a 0.01-Sv (1-rem) dose limit for both safety and security events at the site area boundary.

3. Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., 0.05 Sv (5 rem)), but apply it at the site area boundary instead of at the controlled area boundary. (Changes to ISFSI emergency planning requirements —i.e.,

---

[1] The dose criteria in Title 10 of the *Code of Federal Regulations* (CFR) 72.106, "Controlled Area of an ISFSI or MRS," (0.05 Sievert (Sv) [5 rem] total effective dose equivalent; 0.15 Sv [15 rem] to the lens of the eye; 0.5 Sv [50 rem] as either the sum of the deep dose equivalent and any organ dose, or the shallow dose equivalent to the skin or any extremity) are hereinafter referred to as the 0.05-Sv (5-rem) dose limit.

[2] Final rule - 10 CFR Part 72, "Licensing Requirements for the Storage of Spent Fuel In an Independent Spent Fuel Storage Installation." Published in the *Federal Register* (45 FR 74693) on November 12, 1980. See public comment Issues 20 and 21 (at 45 FR 74696 and 74697).

[3] Final rule - 10 CFR Part 72, "Emergency Planning Licensing Requirements for Independent Spent Fuel Storage Facilities (ISFSI) and Monitored Retrievable Storage Facilities (MRS)." Published in the Federal Register (60 FR 32430) on June 22, 1995. See public comment Issues 17 and 25 (at 60 FR 32434 and 32435).

[4] Enclosure 1, "Should a Radiological Acceptance Criterion for Security Scenarios be Applied Consistently to All ISFSIs? (Policy Issue 1)."

the potential to classify events to a "general emergency" level—would likely be required.) or

4. Increase the dose limit for radiological sabotage consistent with the dose limit for reactor DBAs (i.e., 0.25 Sv (25 rem) at the site area boundary). (Changes to ISFSI emergency planning requirements—i.e., the potential to classify events to a "general emergency" level—would be required.)

The staff recommends Option 2. This option provides consistency between the dose limits for ISFSI DBAs and acts of radiological sabotage. Since this paper contemplates ISFSI licensees potentially extending their controlled area boundary outward (to meet a radiological sabotage dose limit), the staff would propose adding a new requirement for licensees to verify doses are also less than 0.01 Sv (1 rem) at the site area boundary. The term "site boundary" is defined in 10 CFR 20.1003 ("Definitions");[5] however, it is not defined in 10 CFR Part 72 or Part 73. Given the differences in the physical location of an ISFSI at the various reactor sites, as well as the presence of ISFSIs located away from any reactor, the staff would seek stakeholder input (as discussed in the Commitments section of the main Commission paper) on applying existing or developing new definitions (and criteria) for defining the term "site boundary" for ISFSIs.

While the staff would apply this verification to both safety and security events, no impacts would be expected for safety events. For security events, certain licensees may have challenges due to the short distance to their controlled area boundary. The options in this paper would provide ISFSI licensees sufficient flexibility to address these challenges. Potential options would include changes to the design of the ISFSI, the use of engineered security features to protect the ISFSI, changes to the ISFSI protective strategy, or changes to the ISFSI emergency planning program. Furthermore, this option would not impact the public health and safety objectives currently contained within the ISFSI's emergency planning program requirements and would continue to support the staff's assumptions that underlie the NRC's 1995 ISFSI emergency planning final rule.

Options 3 and 4 would require reassessment and expansion of the ISFSI emergency planning program requirements, since a foundational assumption from the 1995 ISFSI emergency planning final rule may no longer be valid (i.e., the dose at the site area boundary could exceed the EPA PAGs' dose limit of 0.01 Sv (1 rem)). Should the Commission conclude that Options 3 or 4 are preferable to Option 2, the staff would need to evaluate several safety, legal, policy, and technical issues, including whether a collocated or a non collocated ISFSI's emergency planning program, capable of classifying events at a "general emergency" level, should contain the same elements as a power reactor's emergency planning program to ensure adequate protection of public health and safety. This would include discussions with the U.S. Federal Emergency Management Agency (FEMA) on the applicability of FEMA's regulations to ISFSIs and whether conforming changes to FEMA's offsite emergency planning regulations would also

[5] 10 CFR 20.1003, "*Site boundary* means that line beyond which the land or property is not owned, leased, or controlled by the licensee."

be necessary. The FEMA regulations, which apply to State and local entities, appear to address only "commercial nuclear power facilities."[6]

Background

As discussed in the statements of consideration accompanying the 1980 final rule that initially promulgated 10 CFR Part 72, the current 0.05-Sv (5-rem) dose limit in 10 CFR 72.106(b) was derived from protective actions recommended by the EPA for projected doses to populations for planning purposes. Additionally, under a 1995 ISFSI emergency planning final rule the NRC addressed the issue of security events exceeding the EPA's PAGs. In public comment Issue 25, a commenter had proposed that "… the accident classification system should include the general emergency. This might be necessary in cases of radiological sabotage." The NRC's response stated:

> An essential element of a General Emergency is that "A release can be reasonably expected to exceed EPA Protective Action Guidelines exposure levels off site for more than the immediate site area." As previously discussed, NRC studies have concluded that the maximum offsite dose [from an ISFSI event] would be less than 1 rem [0.01 Sv] which is less than the EPA Protective Action Guidelines.

Although not fully articulated in the statements of considerations accompanying these previous rulemakings, the staff's assumption is that the NRC's establishment of a regulatory structure using a 0.05-Sv (5-rem) dose limit at the controlled area boundary (with a minimum distance of 100 meters), instead of a structure employing a standard using a 0.01-Sv (1-rem) dose limit at the site area boundary (i.e., the owner controlled area boundary), was intended to provide defense in depth or a "margin of prudency" to preventing a "release [that] can be reasonably expected to exceed the EPA Protective Action Guidelines exposure levels off site" of greater than 0.01 Sv (1 rem). Absent this approach, ISFSI licensees would have potentially been required to classify accidents up to the "general-emergency" level. Requiring certain ISFSI licensees to classify accidents to the "general-emergency" level (i.e., non-collocated, specific-license ISFSIs or ISFSIs collocated with decommissioning power reactors) would significantly increase the cost and complexity of the ISFSI licensee's emergency planning program. Moreover, a licensee choosing to make their controlled area boundary contiguous with their site area boundary—to address the radiological sabotage issues discussed in this paper—would also imply that the Commission should also require a licensee to verify that the EPA PAGs' dose limit of 0.01 Sv (1 rem) is met at the site area boundary (i.e., a contiguous controlled area boundary and site area boundary would necessitate the same dose limit).

[6] 44 CFR 350.4, "Exclusions," states, in part, "The regulation in this part applies only to State and local planning and preparedness with respect to emergencies at commercial nuclear power facilities and does not apply to other facilities which may be licensed by NRC ...."

Under 10 CFR 72.32(a), "Emergency plans," non-collocated, specific-license ISFSI emergency plans are required to classify accidents up to the “alert” level. Collocated ISFSIs at operating power reactors are able to address emergencies up to the "general-emergency" level, since the operating power reactor licensee is required to incorporate the ISFSI into the existing collocated power reactor's emergency plan (see 10 CFR 72.212(b)(6)). However, the staff notes that most power reactors undergoing decommissioning promptly seek exemption from the Commission’s power reactor emergency planning regulations. Thus the decommissioning reactor licensee, along with the associated, collocated ISFSI licensee, would only be required to classify emergencies up to the "alert" level.

For spent fuel stored in a dry storage cask—as opposed to spent fuel in an operating reactor's reactor vessel or spent-fuel storage pool—most of the short-lived nuclides have decayed away before the spent fuel is placed in the storage cask. Current approved storage cask designs typically require a minimum decay/cooling time of 5 years before the spent fuel can be stored in the cask. While the staff was mindful of this difference when originally selecting the 0.05-Sv (5-rem) dose limit in 10 CFR 72.106(b) for ISFSIs, the staff was focused on safety scenarios involving direct radiation exposure from the spent fuel, rather than on security scenarios that may involve the release and subsequent uptake of aerosolized spent fuel. The ISFSI security assessments from SECY-06-0045[7] (discussed in Policy Issues 1 and 6) completed by the staff indicated that certain security scenarios may challenge the 0.05-Sv (5-rem) dose limit, mostly due to [redacted] radioactive materials released from a spent fuel dry storage cask. The staff notes that, due to the relative lack of short-lived nuclides, the committed dose accrued from inhalation or ingestion of [redacted] radioactive material after a release from a dry-storage cask is likely to be delivered over a longer period of time (than would be expected from a release from an operating reactor) and is based largely upon the relatively larger presence of transuranic and longer-lived fission-product particulate matter.

<u>Discussion</u>

Any sabotage-related release from an ISFSI would most likely be a prompt event, where any release occurs essentially immediately after the incident, and little (if any) time would exist for the licensee to recommend and then for State officials to initiate offsite protective action recommendations relative to the plume exposure (e.g., sheltering or evacuating). The dose to offsite personnel from the plume exposure would likely occur within a few minutes of a release from the ISFSI and would also terminate within a short time thereafter. This is in contrast to a reactor event, where a release may continue for a significant period of time. Effectively, an ISFSI security event could be considered a "puff" release. Because the bulk of the accrued dose from an ISFSI event would arise largely from inhalation and ingestion of the respirable particles, and not from the direct exposure to particles once they have fallen out of suspension and contaminated the ground, protective action recommendations such as sheltering in place or

[7] SECY-06-0045, “Results of Implementation of the Decisionmaking Framework for Materials and Research and Test Reactor Security Assessments,” ADAMS No. ML060340452, dated March 1, 2006. [Non-public]

evacuating would likely only limit a small portion of the total dose received from most security events analyzed by the staff in the ISFSI security assessments.

To minimize risk to public health and safety, a higher dose limit would likely necessitate more robust emergency planning. Choosing a higher dose limit (e.g., the current 0.25-Sv (25-rem) dose limit currently utilized by a power reactor under 10 CFR 50.34(a)(1)(ii)(D)(*1*), "Contents of applications; Technical information,") would clearly require further development of the technical bases and, potentially, a backfit analysis, to be performed during the development of the proposed rule. Additionally, choosing a dose limit at the site area boundary higher than the current NRC assumptions stated in the 1995 ISFSI emergency planning final rule (0.01-Sv (1-rem)) would likely require licensees to be able to classify and respond to emergencies up to the "general-emergency" level.[8]

The staff desires Commission direction on whether to (1) keep an ISFSI 0.05-Sv (5-rem) dose limit for both security events and for safety-related DBAs or (2) to increase the dose limits for security-related events or (3) to apply the dose limits at a different boundary. Increasing the dose limit for terrorist attacks above the dose limit for design-basis accidents represents a shift in Commission policy away from a consistent dose limit for ISFSIs, regardless of the initiating event. Additionally, the staff desires direction on whether licensee verification of a 0.01-Sv (1-rem) dose limit at the site area boundary due to both security events and safety-related DBAs is also appropriate.

Issue 2 Options

1. *Keep the dose limit for radiological sabotage consistent with the dose limit for DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary)*.

   The main advantage to this option is that the 0.05-Sv (5-rem) dose limit is already specified in the regulations as a dose limit for both DBAs for all ISFSIs and for security-related events for non-collocated, specific-license ISFSIs only. Under this option, the cause of the dose is not considered when determining which dose limit must be met; the dose limit is the same regardless of the initiating event. This option also has the advantage of holding all ISFSI licensees to the same dose criteria for security events, regardless of the level of emergency planning at the site. Under Policy Issue 1, all ISFSI licensees would be required to meet the same dose limits.

   However, it is likely that most ISFSIs currently meet the dose requirements at the controlled area boundary for security events—largely because existing ISFSIs are currently loading older, colder fuel (i.e., the licensees are not loading the spent fuel to the design basis limit), and because the distance to their controlled area boundaries are greater than the regulatory minimum of 100 meters (328 feet). Some ISFSI licensees

[8] See *Federal Register* notice 60 FR 32430, public comment Issues 17, 25, 35, and 37 (at 60 FR 32434, 32435, 32436, and 32437).

may need to expend additional resources to meet the 0.05-Sv (5-rem) dose limit by increasing the current distances from their ISFSI to the controlled area boundary, or through implementation of other security measures.

The main disadvantage of this option is the potential cost to some ISFSI licensees who have not been subject to the dose limit for security scenarios, and whether or not such a change could be justified for any ISFSI licensee under the backfit rule. [redacted] (see Enclosure 6 to this paper),[9] the staff cannot say, [redacted], whether all ISFSI licensees would also meet a 0.05-Sv (5-rem) dose limit controlled area boundary. The staff notes that some licensees may have limited ability to expand the distance between their ISFSI and the controlled area boundary because of natural, site, or public features.

Since this paper contemplates ISFSI licensees potentially moving their controlled area boundary outward (as an option to meet the security assessments contemplated by this paper under Policy Issue 1), an additional significant disadvantage is whether a licensee would also meet the EPA PAGs of 0.01 Sv (1 rem) at the site area boundary (an underlying assumption from the Commission's 1995 ISFSI emergency planning final rule). The staff has not evaluated whether any ISFSI licensees can meet the 0.01-Sv (1-rem) dose limit at the site area boundary for either DBAs or radiological sabotage events. However, the staff would not expect any impacts for safety-related DBAs. The staff notes that licensees would be provided sufficient flexibility to evaluate the tradeoffs of increased security costs versus increased emergency planning costs in meeting security requirements by setting the distance to the controlled area boundary and thus meeting the 0.05-Sv (5-rem) dose limit.

2. *Keep the dose limit for radiological sabotage consistent with the dose limit for DBAs (i.e., a 0.05-Sv (5-rem) dose limit at the controlled area boundary; and also meet a 0.01-Sv (1-rem) dose limit for both safety and security events at the site area boundary.*

The advantages of Option 2 are the same as Option 1, that is the application of a single 0.05-Sv (5-rem) dose limit that is already specified in the regulations as a dose limit for both DBAs for all ISFSIs and for security-related events for non-collocated, specific-license ISFSIs only. As with Option 1, the cause of the dose is not considered when determining which dose limit must be met; the dose limit is the same regardless of the initiating event. An additional advantage is that licensee verification of a 0.01-Sv (1-rem) dose limit at the site area boundary would confirm the Commission's underlying assumption in the 1995 ISFSI emergency planning final rule. This option would reduce emergency planning uncertainties if an ISFSI licensee moved their controlled area boundary outward to meet a radiological sabotage dose limit. Accordingly, the staff

---

[9] Enclosure 6, "Response to ISFSI Security Questions." [Non-public]

would add a requirement for a licensee to also verify that the dose at the site area boundary is less than the EPA PAGs of 0.01 Sv (1 rem).

As with Option 1, the staff also notes that some licensees may have limited ability to expand the distance between their ISFSI and the controlled area boundary because of natural, site, or public features. Therefore, licensees would be provided sufficient flexibility to evaluate the tradeoffs of increased security costs versus increased emergency planning costs in setting the distance to the controlled area boundary and thus meeting the 0.05-Sv (5-rem) and 0.01-Sv (1-rem) dose limits.

The main disadvantages of this option are the same as Option 1, i.e., the potential cost to some ISFSI licensees who have not been subject to the dose limit for security scenarios, and whether or not such a change could be justified for any ISFSI licensee under the backfit rule. Another disadvantage of this option is that it imposes a verification of the dose at the site area boundary due to DBAs (i.e., a licensee verification that doses are less than 0.01 Sv (1 rem)). However, the staff's expectation is that all ISFSI licensees currently meet this dose limit for DBAs. Additionally, whereas an uncertainty on whether an ISFSI licensee can meet the 0.01-Sv (1-rem) dose limit at the site area boundary would be considered a disadvantage under Option 1, the certainty of meeting the EPA PAGs at the site area boundary and consistency with the Commission's assumptions stated in the 1995 ISFSI emergency planning final rule are considered a significant advantage.

The staff notes that while the term "site boundary" is defined in 10 CFR Part 20 (see § 20.1003), it is not defined in 10 CFR Part 72 or Part 73. Given the differences in the physical location of an ISFSI at the various reactor sites, as well as the presence of ISFSIs located away from any reactor, the staff would seek stakeholder input (as discussed in the Commitments section of the main Commission paper) on applying existing or developing new definitions (and criteria) for defining the term "site boundary" for ISFSIs. This would address the potential range of ISFSIs, e.g., ISFSIs located at an operating reactor, at a decommissioning reactor, or away from any reactors.

3. *Keep the dose limit for radiological sabotage consistent with the dose limit for ISFSI DBAs (i.e., 0.05 Sv (5 rem)), but apply it at the site area boundary instead of at the controlled area boundary. (Changes to ISFSI emergency planning requirements —i.e., the potential to classify events to a "general emergency" level—would likely be required.)*

The main advantage to this option is that the onsite dose limit for both ISFSI safety and security events would remain at 0.05 Sv (5 rem). Additionally, licensees would have more flexibility in meeting the radiological sabotage performance objective by permitting the controlled area boundary to be extended to the site area boundary (i.e., the two boundaries could be contiguous). However, because the dose beyond the site boundary would then be greater than the EPA PAGs of 0.01 Sv (1-rem), licensees would

be required to classify accidents up to the "general emergency" level to ensure that public health and safety are adequately protected.

As discussed in the background section above, most off-site protective action recommendations would serve to limit only the direct dose and the dose from exposure to contaminated ground, not from the dose accrued from plume exposure (i.e., inhalation of respirable radioactive material). This is different from the planning assumptions for protective actions from a radioactive release at an operating power reactor, where the potential for a release to continue for several days must be considered. Consequently, further staff evaluation would be required to identify the scope of the emergency planning program requirements that would be appropriate to this class of licensee and class of events. For example, would an offsite emergency operations facility, a 10-mile emergency planning zone, and a joint information center, etc. be necessary? The staff would need to initiate discussions with FEMA on the applicability of FEMA's regulations to ISFSIs and whether conforming changes to FEMA's offsite emergency planning regulations would also be necessary. The FEMA regulations, which apply to State and local entities, appear to address only "commercial nuclear power facilities," which may not include ISFSIs.

For general-license ISFSIs or collocated, specific-license ISFSIs located at an operating power reactor, an increase in ISFSI emergency planning requirements would likely be enveloped by existing power reactor emergency planning requirements. For non-collocated, specific-license ISFSIs and for ISFSIs located at decommissioning power reactors, increased emergency planning requirements would arise or would be reinstated, respectively (i.e., many decommissioning power reactor licensees seek exemption from the full emergency planning requirements soon after they permanently cease operations, e.g., only requiring the classification of accidents to the "alert" level).

Accordingly, the main disadvantages from this option would be increased potential dose to the public as a result of a terrorist attack at an ISFSI. To mitigate the increased potential dose to the public, non-collocated, specific-license ISFSIs and ISFSIs located at decommissioning power reactors would need to increase their emergency planning requirements. This would create a new or renewed cost, respectively, for these licensees. Rescinding a previously approved exemption for a power reactor licensee (e.g., a decommissioned reactor who had reduced the classification level of their emergency plan upon decommissioning) would likely involve a backfit assessment.

4. *Increase the dose limit for radiological sabotage consistent with the dose limit for reactor DBAs (i.e., 0.25 Sv (25 rem) at the site area boundary). (Changes to ISFSI emergency planning requirements—i.e., the potential to classify events to a "general emergency" level—would be required.)*

This option has the advantage of crediting general-license ISFSIs and collocated, specific-license ISFSIs at operating power reactors for having more robust emergency

planning in place. Additionally, this option has the advantage of allowing ISFSI licensees greater flexibility than Option 1, 2, or 3 for security-related events. For example, this option would not have as much potential for forcing a licensee to extend their controlled area boundaries up to the site area boundary or to implement significantly increased security measures. This would have the effect of reducing the likelihood of a backfit for some licensees.

This option shares many of the disadvantages of Option 3, with respect to a need for increased emergency planning requirements for some ISFSI licensees and discussions with FEMA. Another disadvantage associated with this option is that raising the dose limit for security scenarios above that for DBAs which may have a negative impact on public confidence regarding ISFSIs. Specifically, the public may have difficulty in understanding why a higher dose limit is allowed for a security event, since the health consequences of a given dose are the same, regardless of whether the initiating event is a safety event or a security event.

Additionally, a disadvantage of this option would be the expenditure of significant staff resources to evaluate the legal, regulatory, and technical implications associated with increasing the dose limit for security scenarios. Raising the dose limit criteria for security scenarios above 0.01 Sv (1 rem) at the site area boundary would likely require a higher level of emergency planning than what currently exists at some ISFSIs (e.g., the ability to classify accidents to the "general-emergency" level). Many of the resource impacts under this option are similar to the resource impacts under Option 1, 2, and 3.

Issue 2 Recommendation

The staff recommends Option 2: “Keep the dose limit for security-related events consistent with the dose limit for DBAs (i.e., the 0.05-Sv (5-rem) dose limit); and also meet a 0.01-Sv (1-rem) dose limit for both safety and security events at the site area boundary.” This option would not pose a potential for increased risk to public health and safety, and would therefore not impact the ISFSI's basis for emergency planning, including protective actions' planning. However, this option would provide greater certainty that ISFSI licensees are meetings the EPA PAGs. Additionally, this option provides consistency between dose limits for ISFSI safety-related DBAs and for security-related events, which is consistent with the approach the Commission has taken toward emergency planning at nuclear power reactors.

Should the Design-Basis Threat for Radiological Sabotage Be Applied Consistently to All Independent Spent Fuel Storage Installations (Not Just to General Licensees)? (Policy Issue 3)

Summary

The majority of independent spent fuel storage installations (ISFSIs) licensees (30 of the current 45) are general licensees that are already required to establish a physical protection system which protects the spent fuel against the design basis threat (DBT) for radiological sabotage in accordance with the power reactor security requirements of 10 CFR 73.55.[1] The current regulations and previous staff practice have resulted in regulatory confusion on whether specific-license ISFSIs are required to protect the spent nuclear fuel against the DBT for radiological sabotage. The staff has identified three options for Policy Issue 3:

1. Take no action. Do not require specific licensees to protect against the DBT for radiological sabotage. (The regulations would continue to apply the DBT for radiological sabotage to general-license ISFSIs, but not to specific-license ISFSIs.)

2. Continue to apply the DBT for radiological sabotage to general-license ISFSIs. Additionally, apply the DBT for radiological sabotage to specific-license ISFSIs. (The regulations would apply the DBT for radiological sabotage to all ISFSI licensees.)

   (a) Develop a separate adversary characteristics guidance document for ISFSIs; or

   (b) Retain a single adversary characteristics guidance document (applicable to all classes of licensees subject to the DBT for radiological sabotage) and develop an ISFSI-specific sub-tier document.

3. Develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements (ISFSI licensees would not be required to protect the ISFSI against the DBT for radiological sabotage). Develop ISFSI-specific regulatory guidance supporting the new regulations.

The staff recommends Option 3. While the staff views both Option 2(a) and Option 3 as technically acceptable, and either option would result in an appropriate level of security for ISFSIs, the staff is recommending Option 3 because it does not require developing multiple adversary characteristics documents supporting the singular DBT for radiological sabotage.

The staff would use a "risk-informed, performance based" process to define a new regulatory structure for ISFSI security activities. The "risk-informed" element would apply a vulnerability assessment methodology against ISFSIs that is informed by both the intelligence community's developed threat stream and by vulnerability information that is not threat based (i.e., the

[1] Title 10 of the *Code of Federal Regulations* (CFR) 73.55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage."

evaluation of whether ISFSIs may be vulnerable to certain specific weapons effects for which an underlying threat stream does not currently support their inclusion under the DBT for radiological sabotage). The "performance based" element would apply specific radiological dose acceptance limits to ISFSI security activities. This combined approach would provide flexibility in crafting an appropriate security regulatory structure for ISFSIs that may be different than that used for power reactors and would provide clear and objective performance standards. This new approach would recognize that the security regulatory structure applied to ISFSIs may be appropriately different from the security regulatory structure applied to power reactors, due to significant differences in: (1) the designs of these two types of facilities, (2) the nature of their security vulnerabilities, (3) differences in the physical and regulatory approaches used to create defense-in-depth for these facilities, and (4) differences in the nature and size of a potential radiological release from these facilities. The staff envisions an annual review of threat stream to evaluate whether any changes in the adversary capabilities would differ significantly from the basis for Commission decisions underlying the security assessment frameworks or ISFSI security requirements.

In implementing this option, the staff would support the new regulations by developing a regulatory guidance document that would describe the details of the ISFSI security-related scenarios. Staff recommendations on the scope and content of this guidance document are discussed in Policy Issue 4 (see Enclosure 4 to this paper).[2] The radiological sabotage scenarios described in the regulatory guidance document would enable ISFSI licensees to perform a CARVER-type analysis[3] (see Enclosure 5 to this paper) to determine whether the ISFSI meets the 0.05-Sv (5-rem) dose limit criteria.[4] [5] [6] In recommending this option, the staff additionally recommends continuing the agency's current practice of not performing force-on-force exercises against ISFSIs. Rather, if the staff's recommendations for Policy

---

[2] Enclosure 4, “Should the Regulatory Guidance Supporting the Performance-Based Security Regulations Recommended Under Policy Issue 3 be Bounded by the (Power Reactor) Adversary Characteristics that Support the Design Basis Threat for Radiological Sabotage? (Policy Issue 4).”

[3] C.A.R.V.E.R. analysis includes an evaluation against the following factors: Criticality - identify critical assets; Accessability - determine ease of access to critical assets; Recuperability - compare time to repair, replace, or bypass critical assets; Vulnerability - evaluate security system effectiveness against malevolent capabilities; Effect - consider the scope and consequences of the adverse effects from malevolent acts; and Recognizability - evaluate the potential that adversaries would recognize a critical asset.

[4] Enclosure 5, “Background Information on Threat Assessments and CARVER Analysis.”

[5] The dose criteria in 10 CFR 72.106, "Controlled area of an ISFSI or MRS," (0.05 Sievert (Sv) [5 rem] total effective dose equivalent; 0.15 Sv [15 rem] to the lens of the eye; 0.5 Sv [50 rem] as either the sum of the deep dose equivalent and any organ dose, or the shallow dose equivalent to the skin or any extremity) are hereinafter referred to as the 0.05-Sv (5-rem) dose limit.

[6] As discussed in Policy Issue 2, the staff would recommend a 0.05-Sv (5-rem) dose limit at the controlled area boundary and an additional verification of a 0.01-Sv (1-rem) dose limit at the site area boundary; hereinafter, called the 0.05-Sv (5-rem) dose limit.

Issues 1 and 2 (see Enclosures 1 and 2 to this paper)[7] [8] are approved, the staff would require ISFSI licensees to provide high assurance that a 0.05-Sv (5-rem) dose limit would not be exceeded for a maximally exposed individual at the controlled area boundary as a result of the specified radiological sabotage scenarios (similar to the existing requirements in 10 CFR 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste," for non-collocated, specific-license ISFSIs).

Background

General-license ISFSIs comprise the majority of the current ISFSI licensees (30 out of 45). These general licensees are already required by 10 CFR 72.212(b)(5), "Conditions of general license issued under § 72.210," to establish a physical protection system that protects the spent fuel against the DBT for radiological sabotage, in accordance with physical security requirements for power reactors under 10 CFR 73.55. The current regulation in 10 CFR 72.212(b)(5) requiring general licensees to "[p]rotect the spent fuel against the design basis threat of radiological sabotage in accordance with … § 73.55 …" has been in place since July 1990, when the general-license provisions were added to 10 CFR Part 72.[9]

The current regulations in 10 CFR Part 72 and Part 73, "Physical Protection of Plants and Materials," do not explicitly require the remaining ISFSI licensees (collocated or non-collocated specific-license ISFSIs) to protect their ISFSI against the DBT for radiological sabotage. Staff's historical practice has been to permit specific-license ISFSIs collocated at an operating power-reactor site to comply with the security requirements of 10 CFR 73.55, which does reference the DBT for radiological sabotage (see Figure 1, "Governing Regulations for ISFSI Security Requirements" in the main Commission paper). Additionally, the scope of the DBT for radiological sabotage regulation in 10 CFR 73.1 ("Purpose and scope") does not specifically exclude specific-license ISFSIs. Specific-license ISFSIs do not have any requirements in 10 CFR Part 72 similar to the language in 10 CFR 72.212(b)(5) requiring general-license ISFSIs to protect spent fuel against the DBT for radiological sabotage. Furthermore, the previous regulations in 10 CFR 73.1(a) only exempted specific-license ISFSIs from certain elements of the DBT for radiological sabotage, implying that specific-license ISFSIs were subject to some portion of the DBT for radiological sabotage. However, the Commission in the recent final DBT rule removed any references to specific license ISFSIs from 10 CFR 73.1 and indicated in the Statements of Consideration that the DBT for radiological sabotage did not apply to specific-

[7] Enclosure 1, "Should a Radiological Acceptance Criterion for Security Scenarios Be Applied Consistently To All Independent Spent Fuel Storage Installations? (Policy Issue 1)."

[8] Enclosure 2, "Should the Dose Limits for Acts of Radiological Sabotage (If Any Are Established Under Policy Issue 1) Be the Same as the Dose Limits for Design-Basis Accidents? (Policy Issue 2)."

[9] 10 CFR Part 72, "Licensing Requirements for the Independent Storage of Spent Nuclear Fuel, High-level Radioactive Waste, and Reactor-related Greater than Class C Waste."

license ISFSIs.[10] The final DBT rule was provided to the Commission in SECY 06-0219 and was approved in SRM-M070129.[11]

To address an ambiguity in the regulations, with regard to specific-license ISFSIs, the final DBT rule removed the exemption language from 10 CFR 73.1(a) for specific-license ISFSIs. However, because the final DBT rule was focused on security requirements for power reactors and Category I strategic special nuclear material licensees, the rule changed the scope of 10 CFR 73.1 to not apply the DBT for radiological sabotage to specific-license ISFSIs. The Commission indicated that resolution of (1) the differing security requirements between general-license ISFSIs and specific-license ISFSIs and (2) the applicability of the DBT for radiological sabotage to specific-license ISFSIs would be considered in a future rulemaking.[12] Accordingly, this paper provides a substantive and comprehensive review of the policy and regulatory implications of applying the DBT for radiological sabotage to ISFSIs in preparation for that rulemaking. The Commission's most recent comprehensive reviews of ISFSI security regulations occurred in 1994 and 1998 rulemakings (i.e., the land vehicle bomb rulemaking and the physical protection of spent nuclear fuel rulemaking, respectively).[13] [14]

Despite the different treatment in the regulations of generally-licensed ISFSIs and specifically-licensed ISFSIs, the October 2002 ISFSI security orders issued in response to the terrorist attacks of September 11, 2001—and ISFSI security orders issued to new licensees subsequent to the October 2002 orders—brought all ISFSIs to the same level of protection. Therefore, the staff views the promulgation of clarifying regulations is appropriate within a normal rulemaking process.

---

[10] Final Rule - 10 CFR Part 73, "Design Basis Threat." Published in the *Federal Register* (72 FR 12705) on March 19, 2007. Public comment Issue 5 (at 72 FR 12716).

[11] SECY-06-0219, "Final Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements," Agencywide Documents Access and Management System (ADAMS) No. ML062130289, dated October 30, 2006. SRM-M070129, "Affirmation Session: SECY-06-0219, 'Final Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements,' ADAMS No. ML070290286, dated January 29, 2007.

[12] See *Federal Register* notice 72 FR 12705, public comment Issue 5 (at 72 FR 12716): "… the NRC is currently considering future rulemakings to align the generally-licensed [ISFSI] and specifically-licensed ISFSI requirements and to evaluate the application of the DBT [for radiological sabotage]."

[13] Final rule - 10 CFR Part 73, "Protection Against Malevolent Use of Vehicles at Nuclear Power Plants." Published in the *Federal Register* (59 FR 38889) on August 1, 1994.

[14] Final rule - 10 CFR Parts 60, 72, 73, 74 and 75, "Physical Protection for Spent Nuclear Fuel and High Level Radioactive Waste." Published in the *Federal Register* (63 FR 26955) on May 15, 1998.

Discussion

Since general licensees are presently required to protect the spent fuel against the DBT for radiological sabotage, revising 10 CFR Parts 72 and 73 to ensure consistency between general-license and specific-license ISFSIs would involve either (1) requiring both general- and specific-license ISFSIs to protect against the DBT for radiological sabotage, or (2) requiring both general- and specific-license ISFSIs to comply with new ISFSI-specific, performance-based security requirements and also removing the requirement for general licensees to protect against the DBT for radiological sabotage. Staff views the development of consistent security requirements for all ISFSI licensees as a fundamental policy objective that is necessary for long-term regulatory stability and for maintaining public confidence in the NRC's regulatory program.

To facilitate discussion of the options for this policy issue, staff would first discuss the proposed meaning applied to the phrase “protecting against the DBT for radiological sabotage” (as it applies to ISFSI licensees). Additionally, staff would address, when appropriate, performing force-on-force exercises at an ISFSI licensee subject to the DBT for radiological sabotage. And lastly, to address the goal of preserving the general-license process, staff would discuss how the proposed options impact the need for ISFSI licensees to submit their security plans to the NRC for prior review and approval.

Protecting Against the DBT

A consideration associated with this policy issue is the meaning of the phrases “protecting spent fuel against the DBT for radiological sabotage,” and/or “applying the DBT for radiological sabotage.” For power reactors, protecting the reactor facility against the DBT for radiological sabotage has typically meant that the personnel and security systems respond to the threat elements under the DBT by interposing security personnel and/or engineered barriers between the adversaries and critical target-set equipment. The security personnel are then required by the current 10 CFR 73.55(h)(4)(iii)(A) to prevent or impede attempted acts of radiological sabotage (i.e., the implementation of a "denial of task" protective strategy).

However, under 10 CFR 72.212(b)(5)(v), general-license ISFSIs are currently exempt from the requirement to prevent or impede attempted acts of radiological sabotage required by 10 CFR 73.55(h)(4)(iii)(A) for power reactors. Additionally, non-collocated, specific licensees are currently required by 10 CFR 73.51(b)(3) to establish and maintain a physical protection system that “must be designed to protect against loss of control of the facility that could be sufficient to cause a radiation exposure exceeding...[the 0.05-Sv (5-rem) dose limit at the controlled area boundary].” Therefore, with respect ISFSIs, the staff would propose to interpret “protecting spent fuel against the DBT for radiological sabotage” to mean that for an ISFSI licensee a particular dose limit should not be exceeded if an act of radiological sabotage were to occur.

If the Commission agrees with the staff's recommendations for Policy Issues 1 and 2, the staff would interpret the phrase "protecting against the DBT for radiological sabotage" (and "applying the DBT for radiological sabotage to ISFSI licensees") to mean that an ISFSI licensee's physical security system would be required to provide high assurance that a terrorist attack on an ISFSI would not result in a radiological release with the potential to cause a dose exceeding the 0.05-Sv (5-rem) dose limit to a maximally exposed individual located at the ISFSI's controlled area boundary.

Force-on-Force Exercises

Currently, the staff does not conduct force-on-force (FOF) security exercises against ISFSIs. The staff evaluated whether this practice should continue. In the ISFSI security assessments in SECY-06-0045,[15] the staff concluded that ■■■■■■■■■■■■■■■■■■■■■ the potential exists for certain malevolent acts to breach a storage cask's confinement boundary (see discussion in Enclosure 6).[16] However, a large number of site-specific variables (e.g., distance from the ISFSI to the controlled area boundary, cask design, spent fuel loading patterns inside the cask, cask placement on the storage pad, spent fuel characteristics, weapons capabilities, etc.) impact the resulting dose at the licensee's controlled area boundary. Therefore, the potential to breach a cask's confinement boundary does not necessarily indicate that the 0.05-Sv (5-rem) dose limit would be exceeded at the ISFSI's controlled area boundary, or that the licensee is unable to protect the ISFSI against the DBT for radiological sabotage.

For example, licensees with a large distance from the ISFSI to their controlled area boundary (and/or licensees that store older, colder, fuel; etc.) would be able to balance the necessary protective strategy requirements for the ISFSI against the potential dose at the controlled area boundary caused by radiological sabotage. Therefore, such ISFSI licensees could retain their current protective strategy and thus continue to provide high assurance that the potential dose at the controlled area boundary from an act of radiological sabotage would remain less than the prescribed dose limit. However, ISFSI licensees with limited distances to their controlled area boundaries, or with other constraints (e.g., high-burnup fuel), may have to revise their protective strategy, revise the ISFSI's design, or use engineered features to provide the requisite high assurance that the licensee's physical protection system would protect the ISFSI against the DBT for radiological sabotage and thus meet the 0.05-Sv (5-rem) dose limit.

If the performance measure for ISFSIs is to ensure that the 0.05-Sv (5-rem) dose limit is not exceeded as a result of attempted acts of radiological sabotage, rather than to prevent or impede acts of radiological sabotage, then it is logical to question the usefulness of testing ISFSI licensees with FOF exercises. To date, FOF exercises have not been conducted at

[15] SECY-06-0045, "Results of Implementation of the Decisionmaking Framework for Materials and Research and Test Reactor Security Assessments," ADAMS No. ML060340452, dated March 1, 2006. [Non-public]

[16] Enclosure 6, "Response to ISFSI Security Questions." [Non-public]

ISFSIs. Furthermore, both prior and current FOF exercises have excluded general-license ISFSIs and collocated specific-license ISFSIs from the scope of power reactor FOF exercises.

Consequently, the staff's view is that there would be minimal benefit to be gained from performing FOF exercises at ISFSI licensees, [redacted] implement a detect, assess, and communicate protective strategy (as opposed to a "denial of task" protective strategy). ISFSI licensees that ensure that the dose limit is not exceeded by relying upon the distance to the controlled area boundary (and any other necessary protective measures) and the response of offsite law enforcement personnel, would not need to demonstrate how the security staff would defend against the attacking FOF personnel. Instead of performing a FOF exercise, the staff can verify, through inspection, that the licensee's security plans require local law enforcement authorities to be contacted and that the response time is adequate.

Additionally, the recently added section 170D.a of the AEA,[17] mandates that "… the Commission shall conduct security evaluations at each licensed facility that is part of a class of licensed facilities, as the Commission <u>considers</u> to be appropriate, to assess the ability of a private security force of a licensed facility to defend against any applicable design basis threat." (emphasis added). Additionally, section 170D.b of the AEA mandates that "[t]he security evaluations shall include force-on-force exercises." The staff's view is that section 170D.a provides the Commission with the necessary flexibility to consider whether FOF exercises are appropriate for a general- or specific-license ISFSIs, if that class of licensees is required to defend against the DBT for radiological sabotage.

Therefore, for all of the options discussed under this policy issue, staff does not recommend performing FOF exercises at ISFSIs subject to the DBT for radiological sabotage when the ISFSI is implementing a detect, assess, and communicate protective strategy. [redacted] ISFSI licensees use a detect, assess, and communicate protective strategy, whether they are a general-license ISFSI or a collocated or non-collocated specific-license ISFSI. However, if an ISFSI licensee's analysis under Options 2 or 3 indicated that a "denial of task" protective strategy is necessary to meet the 0.05-Sv (5-rem) dose limit, then staff would evaluate, on a case-by-case basis, whether FOF exercises are appropriate for that particular licensee.

Licensee Submittal of Security Plans for NRC Prior Review and Approval

Regardless of which options the Commission chooses with this policy issue, when combined with the recommendations for Policy Issues 1 and 2 to use a dose-based acceptance criteria, the staff notes that some ISFSIs may be compelled to revise their current protective strategy from a "detect, assess, and communicate" protective strategy to a "denial of task" protective strategy, due to site-specific limitations. [redacted]. However, staff's view is that if an ISFSI licensee were to implement a "denial of task" protective strategy, that licensee would be required to submit their security

---

[17] Section 170D was added to the Atomic Energy Act of 1954 (AEA) under section 651(a) of the Energy Policy Act of 2005 (EPAct) (42 U.S.C. 2201d).

plans to the NRC for prior review and approval. For a specific-license ISFSI, NRC prior review and approval of security plans is required under the current regulations. For a general-license ISFSI, the security requirements for the ISFSI are incorporated in the security plan (required under Part 50) for the associated power reactor license and are subject to inspection by NRC regional staff. Reactor licensees are permitted under 10 CFR 50.54(p)(1), ("Conditions of Licenses"), to make certain changes to their security plan without prior NRC review and approval, provided such changes do not decrease the effectiveness of their security plan. In all likelihood, a general-license ISFSI's shift to a denial protective strategy would not decrease the effectiveness of the associated power reactor's security plan under 10 CFR 50.54(p)(1).

The use of a "denial of task" protective strategy raises issues of sufficient technical complexity to necessitate prior staff review and approval of a licensee's security plan. The staff bases this conclusion on (1) experience gained in the CY 2003 - CY 2004 reviews of changes to reactor security plans to implement the security and DBT orders and the resultant degree of complexity and the need for interactions with licensees, and (2) a desire to maintain an appropriate independence and separation of NRC security plan review and approval and inspection functions. For a specific-license ISFSI, NRC prior review and approval of applicant's initial security plans is required under the current regulations. Under 10 CFR 72.44(e), ("License conditions"), licensees may make certain changes to their security plan without NRC prior review and approval, if such changes do not decrease the effectiveness of the security plan. For a general-license ISFSI, the security requirements for the ISFSI are incorporated in the security plan (required under Part 50) for the associated power reactor license and are subject to inspection by NRC regional staff, not to staff prior review and approval. Similarly, reactor licensees are permitted under 10 CFR 50.54(p)(1), ("Conditions of licenses"), to make certain changes to their security plan without prior NRC review and approval, provided such changes do not decrease the effectiveness of their security plan. In all likelihood, a general-license ISFSI's shift to a denial protective strategy would not decrease the effectiveness of the associated power reactor's security plan under 10 CFR 50.54(p)(1).

Issue 3 Options

1. *Take no action. Do not require all specific licensees to protect against the DBT for radiological sabotage. (The regulations would continue to apply the DBT for radiological sabotage to general licensees, but not to specific licensees.)*

   This option has been included only for completeness of analysis. If this option were adopted, the DBT for radiological sabotage would continue to apply to general licensees, but would not apply to all specific licensees. The only advantage to this option is that it does not require additional staff time and resources; however, the staff's effort for the rulemaking to revise ISFSI security requirements has already been evaluated and budgeted, as discussed in COMSECY-05-0058.[18]

[18] COMSECY-05-0058, "Schedules and Resources for Security Rulemakings," ADAMS No. ML060390479, dated November 30, 2005. [Non-public]

The main disadvantage is that regulatory consistency would not be maintained for spent fuel stored at a specific-license ISFSI as compared to a general-license ISFSI. This would yield different regulatory treatment for storing the same radioactive material (spent fuel) in the same storage cask designs at different locations. Additionally, this option would not provide a set of scenarios for the licensees to analyze to determine compliance with the 0.05-Sv (5-rem) dose limit as recommended under Policy Issues 1 and 2. Furthermore, this option is inconsistent with the Commission's fundamental approach taken in the October 2002, ISFSI security orders, which applied the same security requirements to all ISFSI licensees. Under this option, making the requirements in the ISFSI security orders generically applicable to all ISFSIs would not be possible.

The staff's view is that continuing differences between general-license and specific-license ISFSI security requirements is not appropriate and does not contribute to long-term regulatory stability or to stakeholder support and understanding of the Commission's regulatory programs for storing spent fuel.

2. *Continue to apply the DBT for radiological sabotage to general-license ISFSIs. Additionally, apply the DBT for radiological sabotage to specific-license ISFSIs. (The regulations would apply the DBT for radiological sabotage to all ISFSI licensees.)*

This option continues to require general-license ISFSIs to protect against the DBT for radiological sabotage. Additionally, this option requires revising the existing physical security requirements for both collocated and non-collocated specific-license ISFSIs in 10 CFR 73.51 with a requirement for these licensees to protect spent fuel or high-level radioactive waste against the DBT for radiological sabotage. Conforming changes would also be made to 10 CFR 72.180, "Physical protection plan," and 72.182, "Design for physical protection," to clarify that specific licensees are required to protect the spent fuel or high-level radioactive waste against the DBT for radiological sabotage. The new regulations would require ISFSI licensees to provide high assurance that the 0.05-Sv (5-rem) dose limit would not be exceeded at the controlled area boundary, and that the 0.01-Sv (1-rem) dose limit would not be exceeded at the site area boundary, as a result of a malevolent act described in the DBT for radiological sabotage. This approach would be similar to the approach taken in 10 CFR 73.51 for specific-license ISFSIs.

Additionally, the staff would propose applying the waterborne vehicle bomb assault element of the recently approved DBT rule to ISFSIs. Under the recent final DBT rule,[19] all ISFSIs are exempt from the waterborne vehicle bomb assault requirement. ■■■■■■■ ■■■■■■■■■■■■■■ this is not a concern since the land vehicle bomb assault requirement typically envelopes an ISFSI site on a 360-degree basis. ■■■■■■■■■■■■■■■■■■■■ this is not the case and a waterborne vehicle bomb assault is a possibility. Therefore, the staff would propose subjecting all ISFSIs to the waterborne vehicle bomb assault threat.

[19] See *Federal Register* notice 72 FR 12705 (at 72 FR 12727).

However, the staff would expect most licensees to address this additional threat by an analysis indicating that there are no navigable bodies of water in proximity to the ISFSI, or that analysis of the land vehicle bomb assault threat envelopes the ISFSI on a 360-degree basis; thereby, negating any possible waterborne vehicle bomb assault threat.

This option would hold all ISFSI licensees to the same standard of protection. Currently, both general-license and specific-license ISFSIs have essentially the same physical security systems through the licensees' implementation of the October 2002 ISFSI security orders. With the current ISFSI security orders in place, this option would impose practically no significant changes on the licensees' physical security systems for licensees that can meet the 0.05-Sv (5-rem) dose limit.

This option is advantageous because it would be consistent with the current regulations which require general-license ISFSIs to protect against selected elements of the DBT for radiological sabotage. That requirement has been in place for more than a decade. Applying the DBT for radiological sabotage to both general-license and specific-license ISFSIs would provide the greatest consistency with the Commission's historical regulatory approach for this class of licensees. Furthermore, because the DBT for radiological sabotage would remain applicable to general licensees, this option is likely to have stakeholder support.

Applying the DBT for radiological sabotage to all ISFSIs would also be advantageous because licensees would be able to evaluate a set of threat scenarios against their ISFSI when determining regulatory compliance with the 0.05-Sv (5-rem) dose limit for security-related events. As a performance-based approach, this option would give licensees flexibility in developing security solutions best suited for their specific facility. For example, the licensee would evaluate the design of the ISFSI (e.g., cask design, spent fuel burnup and decay time, cask loading patterns, distance to the controlled area boundary, etc.) against the DBT for radiological sabotage and supporting regulatory guidance and then would calculate the potential dose consequences, if any, resulting from an attack. Based upon the results, the licensee would best determine what changes, if any, are necessary (e.g., changes to the design of its ISFSI, the distance to the controlled area boundary, or the licensee's physical security plans) to provide the requisite high assurance that the licensee can meet the 0.05-Sv (5-rem) dose limit at the controlled area boundary. Licensees who already meet the 0.05-Sv (5-rem) dose limit would not need to make any changes to the design of the ISFSI, to the physical security system, or to the protective strategy.

A potential disadvantage to applying the DBT for radiological sabotage to ISFSIs is that the ISFSI rulemaking would potentially subject the DBT regulations to the same challenges received during the recent DBT rulemaking.

If this option were selected by the Commission, the staff would also develop a regulatory guidance document specifying the adversary characteristics that are applicable to

ISFSIs. Staff has identified two approaches to developing the guidance document: (a) developing a separate ISFSI adversary characteristics regulatory guidance document, or (b) applying the existing radiological sabotage adversary characteristics regulatory guidance to ISFSIs, and then developing an ISFSI-specific, sub-tier guidance document to indicate which portions of the existing guidance apply to ISFSIs.

(a) Develop a separate adversary characteristics guidance document for ISFSIs.

This option would require the staff to develop a separate, ISFSI-specific adversary characteristics regulatory guidance document. Staff views this option as a logical extension of the regulatory structure approved by the Commission under the recently approved final DBT rulemaking and the currently underway proposed power reactor security rulemaking.[20] Specifically, this regulatory structure includes the use of a performance-based DBT and licensee-class specific security regulations, combined with supporting regulatory guidance documents that are controlled as safeguards or classified information. This structure provides the Commission with flexibility in addressing future changes to the threat environment or in addressing changes to potential vulnerabilities through changes to regulatory guidance documents, rather than through rulemaking or orders. Additionally, this structure supports an appropriate degree of information security on adversary characteristics (or vulnerability) information (i.e., need to know). For example, the use of a separate ISFSI-specific guidance document would limit the cask certificate holders' access to power reactor adversary characteristics, if the certificate holder was performing the dose calculations described in Policy Issue 1 (see Enclosure 1 to this paper), on behalf of the ISFSI licensee.

A main disadvantage would be the inherent complexity, and potential for stakeholder confusion, of having multiple adversary characteristics regulatory guidance documents associated with the single DBT for radiological sabotage. Another disadvantage is the staff resources necessary to develop the ISFSI-specific guidance document.

(b) Retain a single adversary characteristics guidance document (applicable to all classes of licensees subject to the DBT for radiological sabotage) and develop an ISFSI-specific sub-tier document.

The principal advantage of this option is that it retains a single adversary characteristics document for the DBT for radiological sabotage—for all classes of licensees subject to the DBT for radiological sabotage. However, as with Option 2(a), this option would require the development of additional documents. Specifically, this option would require staff to develop an ISFSI-specific, sub-tier guidance document to define the specific components of the overall adversary characteristics that are applicable to ISFSIs, and,

[20] SECY-05-0106, "Proposed Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements," ADAMS No. ML050530109, dated June 14, 2005, published in the *Federal Register* (70 FR 67380) on November 7, 2005 (at Section VI, page 70 FR 67386). SECY-06-0126 (at Section V, page 70 FR 62482).

possibly, to include information that is not included in the overall adversary characteristics guidance document.

A major disadvantage associated with this option is the inherent complexity and potential for confusion among licensees and other stakeholders who would have to refer to multiple documents (i.e., the adversary characteristics document associated with the DBT for radiological sabotage and an additional, ISFSI-specific guidance document). Additionally, this option may require more resources than would be required by Option 2(a) to address future changes to these guidance documents (i.e., rather than revising one document, the staff would have to potentially change multiple documents).

Creating sub-tier guidance documents that are derived, but differ, from parent guidance documents would be burdensome to both the staff and the licensee. Finally, the use of a compilation and variation approach could result in increased risk of disclosure of safeguards and/or classified information between reactor licensees and non-reactor licensees. For example, an ISFSI licensee may need the assistance of a cask certificate holder (vendor) to perform the necessary vulnerability evaluations, which would result in a need to share the overall adversary characteristics document as well as the sub-tier guidance document with the certificate holder, who would otherwise not have a need to know the information in the adversary characteristics for power reactors).

3. *Develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements (ISFSI licensees would not be required to protect the ISFSI against the DBT for radiological sabotage). Develop ISFSI-specific regulatory guidance supporting the new regulations.*

This option requires replacing the requirements in 10 CFR Parts 72 and 73 for general-license ISFSIs in order to protect against the DBT for radiological sabotage in 10 CFR 73.1 with new risk-informed, performance-based, security requirements for radiological sabotage for all ISFSI licensees. This approach would also replace the existing physical security requirements for non-collocated specific-license ISFSIs in 10 CFR 73.51, and for collocated specific-license ISFSIs as well, with new, risk-informed, performance-based requirements. The new regulations would require all ISFSI licensees to provide high assurance that the 0.05-Sv (5-rem) dose limit would not be exceeded for a maximally exposed individual at the controlled area boundary for a specified set of radiological sabotage scenarios—similar to the existing regulations in 10 CFR 73.51 for specific-license ISFSIs. Additionally, the staff would develop the new, performance-based security requirements for ISFSIs from a vulnerability perspective, rather than a threat perspective. Options associated with the scope and content of this regulatory guidance is contained in Policy Issue 4 (see Enclosure 4 to this paper). The radiological sabotage scenarios would be described in a supporting regulatory guidance document that would be controlled as safeguards or classified information. This regulatory guidance would enable ISFSI licensees to perform a CARVER-type analysis

(see Enclosure 5 to this paper) to determine whether the ISFSI meets the 0.05-Sv (5-rem) dose limit criteria. The staff views the CARVER methodology as an acceptable, iterable framework for accomplishing such dose assessments and evaluating changes to a security program.

Should the licensee's analysis indicate that the 0.05-Sv (5-rem) dose limit would be exceeded at the controlled area boundary, the licensee would be required to modify one or more aspects of their physical security system and/or the ISFSI's design. Such changes could potentially include, but are not limited to, extending the distance from the ISFSI to the controlled area boundary, modifying cask fuel loading patterns, locating fuel based upon burnup and decay time, modifying the location of casks on the ISFSI storage pad, using engineered barriers or natural features as part of the security system, or changing the licensee's protective strategy. The licensee's completed analysis would either be available for inspection, or submitted to the NRC for review and approval, as appropriate (see prior discussion on licensee's submission of security plans). This approach would (1) provide ISFSI licensees with a significant degree of flexibility in crafting a physical security system that addresses any unique aspects of their ISFSI, and (2) result in the licensee's implementation of a physical security system that meets a consistent regulatory success standard (i.e., the 0.05-Sv [5-rem] dose limit).

This option, as with Option 2, would hold all ISFSI licensees to the same standard of protection. With the current ISFSI orders in place, this option would also impose practically no significant changes on the licensees' physical security programs—assuming that licensees can meet the 0.05-Sv (5-rem) dose limit. A major advantage of this option is that it yields a performance-based regulatory structure informed by licensee-performed, vulnerability- or risk-based analysis and assessment.

The primary disadvantage is that adopting this option would represent a reversal of the longstanding (more than a decade) Commission regulatory position of applying the DBT for radiological sabotage to general-license ISFSIs. As noted above, 30 of the current 45 ISFSIs are general licensees, and all of the projected ISFSI licensees (based upon industry's advance projections to the staff) would use the Part 72 general license. External stakeholders may view removing the requirement for general-license ISFSIs to protect against the DBT for radiological sabotage as a reduction in the security required to store spent nuclear fuel. The staff does not view this action as such, but does recognize that the NRC would have to clearly communicate that the DBT for radiological sabotage requirements are being replaced with a technically sound, graded, risk-informed, performance-based approach to security that provides an equivalent level of security, while recognizing the unique set of factors that must be taken into account when evaluating the security of an ISFSI. In fact, the staff's view is that the adoption of a risk-informed, performance-based regulatory structure provides an equivalent level of security and may provide a firmer technical basis to conclude that the security of an ISFSI was acceptable in providing high assurance of public health and safety.

An additional communication issue to overcome under this option may be an incorrect perception by stakeholders that the NRC is reversing direction shortly after issuing the final DBT rule. For example, the final DBT rule, while removing the applicability of the DBT for radiological sabotage to specific-license ISFSIs, expanded the elements of the DBT that were applicable to general-license ISFSIs by including the existing land vehicle bomb assault threat and the new cyber threat. However, the revisions to 10 CFR 73.1 language affecting general-license ISFSIs were not the focus of the DBT rulemaking, but were instead a conforming change to address part of the October 2002 ISFSI security orders. However, the NRC indicated in the final DBT rule that resolution of (1) the differing security requirements between general-license ISFSIs and specific-license ISFSIs and (2) the applicability of the DBT for radiological sabotage to specific-license ISFSIs would be considered in a future rulemaking.[21]

Another disadvantage of this option is that more resources would likely be necessary to develop the performance-based regulations than would be needed for simply extending the applicability of the DBT for radiological sabotage to include specific-license ISFSIs, as in Option 2. Additional resources would be necessary due to the greater technical and regulatory complexity of the rulemaking, and also due to the need for additional communication with stakeholders. The staff notes that the same resources would be expended to create the supporting regulatory guidance document for either this option or Option 2(a).

Issue 3 Recommendation

The staff recommends Option 3, "Develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements (ISFSI licensees would not be required to protect the ISFSI against the DBT for radiological sabotage). Develop ISFSI-specific regulatory guidance supporting the new regulations." Both Options 2(a) and 3 would achieve the staff's goals for this rulemaking. Both options are performance-based, both achieve technically acceptable levels of security, and both provide flexibility to ISFSI licensees. However, the staff prefers Option 3, because (1) the staff views creation of a risk-informed, performance-based security regulatory structure as providing the greatest support to the Commission's strategic objective of developing performance based regulations by allowing licensees to tailor their security programs and protective measures to the circumstances specific to their ISFSI, while providing the requisite high assurance that the common defense and security will be adequately protected, and (2) the staff does not view the creation of multiple adversary characteristics regulatory guidance documents underlying a singular DBT for radiological sabotage as a vehicle for promoting regulatory clarity.

Additionally, if the Commission approves the staff's recommendation for this policy issue, the staff also proposes early stakeholder engagement in developing the technical bases and proposed ISFSI security rule by making this paper and some of its enclosures publicly available,

[21] See *Federal Register* notice 72 FR 12705, public comment Issue 5 (at 72 FR 12716).

as recommended in Policy Issue 5 (discussed in this Commission paper). Providing stakeholders with an opportunity to better understand the Commission's early thinking during the development of the technical bases and the proposed rulemaking would facilitate constructive and informed dialogue for what would likely be viewed as a significant new regulatory direction on ISFSI security requirements.

Should the Regulatory Guidance Supporting the Performance-based ISFSI Security Regulations Recommended Under Policy Issue 3 Be Bounded by the (Power Reactor) Adversary Characteristics That Support the DBT for Radiological Sabotage? (Policy Issue 4)

Summary

In Policy Issue 3 (see Enclosure 3 to this paper)[1] the staff recommended development of risk-informed, performance-based security regulations that would apply to all independent spent fuel storage installations (ISFSIs) (i.e., both general-license ISFSIs and collocated and non-collocated specific-license ISFSIs), in lieu of applying the design basis threat (DBT) for radiological sabotage under 10 CFR 73.1.[2] The staff also recommended developing a regulatory guidance document supporting these new regulations which would be specific to ISFSIs. This guidance document would be controlled as safeguards or classified information, as appropriate, and would enable ISFSI licensees to perform an analysis of their facilities as described in Policy Issues 1 and 2 (see Enclosures 1 and 2 to this paper).[3] [4]

The regulations currently exempt general-license ISFSIs from some elements of the DBT for radiological sabotage (e.g., waterborne vehicle bomb assault), thereby setting a precedent for requiring ISFSI licensees and power reactor licensees to defend against different adversary capabilities, even though these facilities are collocated. Since no specific regulatory guidance supporting the DBT for radiological sabotage has yet been developed for any ISFSIs, the staff would need to develop guidance for use by both general- and specific-license ISFSIs when demonstrating compliance with the performance-based regulations recommended under Policy Issue 3. This guidance would likely be controlled as Safeguards Information or as classified information. The current adversary characteristics associated with the DBT for radiological sabotage are focused on power reactors. Therefore, the staff is seeking Commission direction on whether the ISFSI security scenarios should be bounded by the adversary characteristics associated with the DBT for radiological sabotage (as applied to operating power reactors). The staff has identified three options for Policy Issue 4:

[1] Enclosure 3, “Should the Design-Basis Threat for Radiological Sabotage Be Applied Consistently to All Independent Spent Fuel Storage Installations (Not Just to General Licensees)? (Policy Issue 3).”

[2] Title 10 of the *Code of Federal Regulations* (CFR) 73.1, "Purpose and scope."

[3] Enclosure 1, "Should a Radiological Acceptance Criterion for Security Scenarios Be Applied Consistently To All Independent Spent Fuel Storage Installations? (Policy Issue 1)."

[4] Enclosure 2, "Should the dose limits for acts of radiological sabotage (if any are established under Policy Issue 1) be the same as the dose limits for design-basis accidents? (Policy Issue 2)."

1. Develop ISFSI regulatory guidance that would be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance would be consistent with the power reactor guidance.)

2. Develop ISFSI regulatory guidance that would not be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance document may include capabilities for which ISFSIs may be vulnerable, but for which power reactors are not.)

3. Develop ISFSI regulatory guidance that would be a combination of Options 1 and 2, depending on the location of the ISFSI. (ISFSIs located away from any power reactors or collocated with a decommissioning power reactor would follow Option 2. ISFSIs collocated with an operating power reactor would follow Option 1 or Option 2, as follows.)

    (a) For collocated ISFSIs (located inside of an operating power reactor's protected area only) the regulatory guidance would be consistent with Option 1. (All other ISFSIs would follow Option 2.); or

    (b) For collocated ISFSIs (located either inside or outside of an operating power reactor's protected area) the regulatory guidance would be consistent with Option 1. (All other ISFSIs would follow Option 2.)

The staff recommends Option 1. This option is consistent with past security requirements for general-license ISFSIs, which were subject to some, but not all, elements of the DBT for radiological sabotage. Overall, this option provides consistent security requirements for protection against radiological sabotage for all ISFSIs, regardless of license type or location. Additionally, this option provides consistency between the scope of the adversary capabilities that both power reactor licensees and ISFSI licensees are required to defend against.

The staff is recommending this option based upon the direction previously provided by the Commission in SRM-SECY-05-0218 on the nature and scope of the adversary characteristics associated with the DBT for radiological sabotage (as applied to operating power reactors).[5] Specifically, options 2 and 3 contemplate ISFSI-specific guidance that is not bounded by the current adversary characteristics regulatory guidance supporting the DBT for radiological sabotage (as applied to operating power reactors).

However, in recommending Option 1, the staff acknowledges that uncertainty exists on whether additional weapons capabilities may pose a vulnerability to spent fuel storage casks. Specifically, the staff acknowledges that an adversary's use of certain types of explosive

[5] SRM-SECY-05-0218, "Semiannual Threat Environment Review," Classified (ADAMS No. not applicable), dated March 30, 2006. [Non-public]

attacks (using either manufactured or improvised devices)—which the Commission has required certain non-reactor licensees, but not ISFSIs, to defend against—may have the potential to breach some cask designs' confinement barrier and thus cause a radiological release that would exceed the 0.05-Sv (5-rem) dose limit at the ISFSI's controlled area boundary.[6] [7]

This uncertainty has only been partially assessed by staff, but would involve, for example, adversaries using explosives to create kinetic, shear, or hydrodynamic weapons effects. The staff has evaluated the use of explosives to create [redacted].[8] [redacted]—which the Commission considers as credible threats for certain non-power reactor licensees—have not been evaluated for ISFSIs. Because of differences between power reactor critical target sets and ISFSI cask designs, the use of explosives to create these weapons effects, by themselves, would not be expected to defeat a power reactor critical target set. [redacted]. Therefore, Option 1 would not resolve these uncertainties [redacted].

Should the Commission conclude that Option 2 or 3 is preferable to Option 1, the staff would recommend assessing additional threat and vulnerability information to support developing the ISFSI-specific regulatory guidance document. Staff would provide the results of the threat and vulnerability evaluation, and any recommendations, to the Commission for its review.

<u>Background</u>

Currently, no ISFSI-specific regulatory guidance has been developed to support either the DBT for radiological sabotage regulations of 10 CFR 73.1 or the ISFSI physical security regulations of 10 CFR 73.51 ("Requirements for the Physical Protection of Stored Spent Nuclear Fuel and High-level Radioactive Waste"). Consequently, the staff will need to develop regulatory guidance for use by ISFSI licensees when they demonstrate compliance with the risk-informed,

---

[6] The dose criteria in 10 CFR 72.106, "Controlled area of an ISFSI or MRS," (0.05 Sievert (Sv) [5 rem] total effective dose equivalent; 0.15 Sv [15 rem] to the lens of the eye; 0.5 Sv [50 rem] as either the sum of the deep dose equivalent and any organ dose, or the shallow dose equivalent to the skin or any extremity) are hereinafter referred to as the 0.05-Sv (5-rem) dose limit.

[7] As discussed in Policy Issue 2, the staff would recommend a 0.05-Sv (5-rem) dose limit at the controlled area boundary and an additional verification of a 0.01-Sv (1-rem) dose limit at the site area boundary; hereinafter, called the 0.05-Sv (5-rem) dose limit.

[8] Enclosure 6, "Response to ISFSI Security Questions." [Non-public]

performance-based regulations recommended under Policy Issue 3 (see Enclosure 3 to this paper).

As discussed in Policy Issue 3, changes to the recent final DBT rule exempts ISFSIs from some elements of the current DBT for radiological sabotage (e.g., the waterborne vehicle bomb assault).[9] Thereby setting a precedent for requiring ISFSI and power reactor licensees to defend against different malevolent attacks. The existing adversary characteristics regulatory guidance supporting the DBT for radiological sabotage (developed as a regulatory guide for power reactors in conjunction with the final DBT rule) originated with the power reactor April 2003 DBT orders, and those orders were focused exclusively on power reactor facilities. Since ISFSI licensees were not included within the scope of the April 2003 DBT orders, no ISFSI-specific weaponry or adversary capabilities are included in the current adversary characteristics regulatory guidance document supporting the DBT for radiological sabotage.

In evaluating this policy issue, the staff does not consider that changes to the existing adversary characteristics supporting the DBT for radiological sabotage (as applied to power reactors) are warranted. Rather, the staff would focus on ISFSI-specific regulatory guidance supporting the risk-informed, performance-based regulations recommended under Policy Issue 3. Consequently, the staff is requesting Commission direction on whether the new, ISFSI-specific regulatory guidance should be consistent with the current "power reactor" adversary characteristics for the radiological sabotage DBT, or whether the guidance should also consider additional appropriate adversary capabilities or ISFSI vulnerabilities.

Discussion

Based upon the results of the ISFSI security assessments in SECY-06-0045,[10] [11] ■■■■■■■■■■■■ ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ vulnerable to attacks using explosives to create certain types of weapons effects which would result in the penetration of some casks' confinement boundary. Staff notes that uncertainty exists on whether the use of these attacks would then create a radiological release from the ISFSI exceeding the 0.05-Sv (5-rem) dose limit at the licensee's controlled area boundary (as recommended under Policy Issues 1 and 2).

This uncertainty has only been partially assessed by staff, but would involve, for example, adversaries using explosives to create kinetic, shear, or hydrodynamic weapons effects against the cask confinement boundary and the spent nuclear fuel contents. The staff has evaluated

---

[9] Final Rule - 10 CFR Part 73, "Design Basis Threat." Published in the *Federal Register* (72 FR 12705) on March 19, 2007.

[10] SECY-06-0045, “Results of Implementation of the Decisionmaking Framework for Materials and Research and Test Reactor Security Assessments,” ADAMS No. ML060340452, dated March 1, 2006.

[11] The staff notes that the consequence measures used in the ISFSI security assessments ■■■■■■■■■■■■■■■■■, consistent with the Commission's direction in SRM-SECY-04-0222, ADAMS No. ML050210288, dated January 19, 2005. [Non-public]

the use of explosives to create [redacted].

Accordingly, the principal question of this policy issue can be distilled into whether it is reasonable and appropriate for the Commission to require licensees to defend their ISFSI against an adversary using explosives in a different manner, or whether it is more appropriate to require licensees to only defend their ISFSI against weapons effects that are bounded by the (power reactor) adversary characteristics associated with the DBT for radiological sabotage. Of importance to this discussion is the fact that because of differences between power reactor critical target sets and ISFSI cask designs, the use of explosives to create these types of weapons effects, by themselves, would not be expected to defeat a power reactor critical target set. [redacted]. The release of this radioactive material may or may not result in a potential dose at the controlled area boundary exceeding the 0.05-Sv (5-rem) dose limit.

In analyzing this issue, a further question arises on whether a specific group of adversaries attacking a single site with different (i.e., multiple) licensed facilities can employ different capabilities to attack one facility or another (i.e., can a licensee with both an ISFSI and a power reactor on a single site be required to defend the ISFSI and the reactor against different adversary capabilities). Almost all (39 out of the existing 45) ISFSIs are collocated with a power reactor (whose status is either operating, undergoing decommissioning, or decommissioned). Eight of the ISFSIs are located at reactors that are undergoing, or have completed, decommissioning. For approximately half of the 39 collocated ISFSIs, the ISFSI is located within an operating power reactor's protected area. The remaining ISFSIs are located within a separate protected area within the reactor site's owner controlled area (i.e., the ISFSI's protected area is separate and distinct from the reactor's protected area).

In evaluating the question of differing adversary capabilities, the staff notes that any NRC regulatory guidance developed to support the proposed security regulations cannot in fact limit what actual tools, weapons, improvised devices, etc. an adversary could employ in an attack (i.e., regulatory guidance cannot practically control what a group of malevolent individuals will or will not do). Instead, this regulatory guidance, which would be controlled as Safeguards Information or classified information, clarifies what the NRC considers reasonable for licensees to defend against—in order to provide the requisite high assurance that public health and safety or the common defense and security will not be unacceptably affected by such an adversary attack.

Consequently, the staff considers differing regulatory guidance (between ISFSIs and power reactors) as an NRC security issue for which the Commission has not previously established a position. Additionally, the staff is not seeking under this policy paper to revise the regulatory guidance applicable to power reactors; but is only seeking Commission direction on whether the ISFSI regulatory guidance should be bounded by the adversary characteristics for the radiological sabotage DBT (as applied to operating power reactors). The staff has developed three options for the Commission's consideration.

Issue 4 Options

1. *Develop ISFSI regulatory guidance that would be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance would be consistent with the power reactor guidance.)*

   Under this option, staff would develop an ISFSI-specific regulatory guidance document that is consistent with the existing adversary characteristics guidance document used by power reactor licensees in applying the DBT for radiological sabotage. The ISFSI regulatory guidance would contain radiological sabotage scenarios (i.e., detailed information) enabling ISFSI licensees to perform assessments demonstrating compliance with the 0.05-Sv (5-rem) dose limit. The contents of the ISFSI guidance document would contain safeguards or classified information, as appropriate. The regulatory guidance developed for ISFSIs under this option would be bounded by the current (power reactor) adversary characteristics supporting the DBT for radiological sabotage. The guidance would not be informed by any additional potential vulnerabilities that may be applicable to ISFSIs, but not to power reactors.

   The principal advantages of this option are: (1) it conforms to the Commission's recent direction in SRM-SECY-05-0218 on the nature and scope of adversary characteristics that are applicable to power reactors, (2) it reduces regulatory confusion for licensees defending both an ISFSI and a power reactor at the same site by applying a single set of adversary characteristics, (3) it treats all ISFSIs the same, and (4) it requires less staff resources to develop a new, ISFSI-specific, vulnerability-informed, regulatory guidance document that is consistent with the power reactor regulatory guidance than to develop regulatory guidance that varies from the current power reactor regulatory guidance.

   The principal disadvantages of this option are: (1) uncertainties would remain regarding whether some ISFSIs are potentially vulnerable to exceeding the 0.05-Sv (5-rem) dose limit if subject to certain weapons effects that are not described in the power reactor guidance, and (2) differences in vulnerabilities between ISFSI cask designs and power reactor critical target set vulnerabilities would not be addressed. Instead this option would continue a "reactor-centric" approach, i.e., the adversary characteristics applied to ISFSIs would be the same as power reactors, whether or not ISFSIs had different vulnerabilities.

2. *Develop ISFSI regulatory guidance that would not be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance document may include capabilities for which ISFSIs may be vulnerable, but for which power reactors are not.)*

   Under this option, staff would develop an ISFSI-specific, risk-informed, regulatory guidance document for ISFSI licensees that may depart from the existing adversary characteristics guidance document used by power reactor licensees in applying the DBT for radiological sabotage. The ISFSI guidance would be informed by the power reactor adversary characteristics regulatory guidance; however, it may include additional adversary capabilities or particular ISFSI vulnerabilities, as appropriate. To support development of this guidance document, the staff would accomplish a risk-informed evaluation to (1) assess ■■■■■■■■■■■■■■■■■■■■■■■■■■ whether their confinement boundary is susceptible to certain weapons effects and (2) identify what weapons effects would be appropriate for an ISFSI licensee to defend against.

   As with Option 1, the ISFSI regulatory guidance would contain radiological sabotage scenarios (detailed information) enabling ISFSI licensees to accomplish the assessments demonstrating compliance with a 0.05-Sv (5-rem) dose limit under the risk-informed, performance-based regulations recommended in Policy Issue 3. The contents of the ISFSI guidance document would contain safeguards or classified information, as appropriate.

   The principal advantages of this option are: (1) uncertainties would be resolved regarding whether ■■■■■■■ ISFSIs are potentially vulnerable to certain weapons effects (i.e., Would a radiological release occur that could result in a dose exceeding the 0.05-Sv (5-rem) dose limit?), (2) all ISFSIs would be treated the same, and (3) differences between ISFSI cask vulnerabilities and power reactor critical target set vulnerabilities would be recognized and addressed.

   The principal disadvantages of this option are: (1) it would not conform to the Commission's direction in SRM-SECY-05-0180 on the nature and scope of adversary characteristics applicable to power reactors, (2) it may create the potential for regulatory confusion by requiring licensees to apply different protective strategies and protective measures in defending ISFSIs and power reactors at the same site (by defending against different weaponry), and (3) it would require additional staff resources to address vulnerabilities specific to ISFSI, rather than follow the current guidance for power reactors. However, the staff notes that some differences currently exist in what a power reactor licensee and an ISFSI licensee are required to defend against, e.g., the waterborne vehicle bomb assault.

3. *Develop ISFSI regulatory guidance that would be a combination of Option 1 and Option 2, depending on the location of the ISFSI. (ISFSIs located away from any power reactors or collocated with a decommissioning power reactor would follow Option 2. ISFSIs collocated with an operating power reactor would follow Option 1 or Option 2, as follows.)*

This option is a variant of Options 1 and 2 above, with the location of the ISFSI (with respect to an operating power reactor) being the determining factor. Under this option, ISFSIs that are located away from any power reactors would apply the regulatory guidance developed under Option 2 above. ISFSIs that are collocated with a decommissioning power reactor would also follow Option 2. ISFSIs that are collocated with an operating power reactor would apply Option 1 or 2 depending upon whether the ISFSI was located inside or outside of the power reactor's protected area. ISFSIs outside of the power reactor's protected area have their own separate protected area.

As discussed in Option 1 above, almost all current ISFSI licensees are collocated with an operating power reactor. Approximately half of these collocated ISFSIs are physically located within their associated power reactor's protected area. The remainder of these collocated ISFSIs are located in their own separate protected area. This separate protected area is still located within the reactor site's owner controlled area. Consequently, and especially for ISFSIs located within the reactor protected area, the question of requiring the same licensee security organization to defend against different adversary capabilities for the ISFSI and the reactor is significant from both a regulatory confusion aspect and from a regulatory burden aspect. However, as noted above significant differences exist between ISFSI vulnerabilities and power reactor critical target set vulnerabilities that would support such a differing approach.

The principal advantage of this option is that it would minimize regulatory confusion between ISFSIs and power reactors. However, the principal disadvantage is that it would not treat all ISFSIs consistently.

This option would apply Option 2 to ISFSIs located away from any power reactor and to ISFSIs collocated with decommissioning power reactors. This option would apply Option 1 or Option 2 to ISFSIs collocated with an operating power reactor as follows:

(a) For collocated ISFSIs (located inside of an operating power reactor's protected area only) the regulatory guidance would be consistent with Option 1. (All other ISFSIs would follow Option 2.); or

This option would require ISFSIs residing in their own separate protected area (whether collocated with an operating power reactor, collocated with a decommissioning power reactor, or away from any power reactor) to apply the regulatory guidance of Option 2. This approach would address the potential ISFSI vulnerabilities of Option 2's guidance

for the greatest number of ISFSIs while minimizing regulatory confusion for operating power reactor licensees.

The principal advantage of this option is that it would minimize regulatory confusion for a number of operating power reactor licensees.

The principal disadvantage of this option is that it would not treat all ISFSIs the same.

(b) For collocated ISFSIs (located either inside or outside of an operating power reactor's protected area) the regulatory guidance would be consistent with Option 1. (All other ISFSIs would follow Option 2.)

This option would require ISFSIs collocated with an operating power reactor to apply guidance that is consistent the power reactor regulatory guidance. ISFSIs collocated with decommissioning power reactors and away from reactor ISFSIs would address potential vulnerabilities under Option 2's guidance.

The principal advantage of this option is that it would minimize regulatory confusion for a greater number of power reactor licensees than Option 3(a).

The principal disadvantage of this option is that it would not treat all ISFSIs the same. Another disadvantage is that a if a power reactor beginning decommissioning and applied for an exemption to reduce its security requirements, this would also affect the ISFSI's security program.

Overall, the staff's view is that Options 1 or 2 are preferable to Option 3 because the staff's goal in this rulemaking is to treat all ISFSIs consistently. This goal outweighs the disadvantage of potential regulatory confusion (i.e., the same licensee being subjected to differing regulatory guidance for their ISFSI and power reactor facilities). However, the recent final DBT rule applied different elements of the DBT to power reactors and to ISFSIs (e.g., waterborne vehicle bomb assaults are not applied to ISFSIs). Therefore, the existence of differing ISFSI and power reactor security requirements would not be inconsistent with current regulations and recent Commission policy choices.

Issue 4 Recommendation

The staff recommends Option 1, "Develop ISFSI regulatory guidance that would be bounded by the adversary characteristics regulatory guidance supporting the DBT for radiological sabotage associated with power reactors. (The ISFSI guidance would be consistent with the power reactor guidance.)" This option is most consistent with past security requirements for general-license ISFSIs, which were subject to some, but not all, elements of the radiological sabotage DBT. This option is most consistent with the Commission's direction in SRM-SECY-05-0218 on the nature and scope of adversary characteristics applicable to power reactors. This option provides consistent security requirements for protection against

radiological sabotage for all ISFSIs, regardless of license type or location. Additionally, this option provides consistency between the security requirements for protection against radiological sabotage for ISFSIs and the security requirements for reactors. Option 1 would also require less staff resources to implement.

Should the Commission conclude that Options 2 or 3 are preferable to Option 1 because of the current uncertainties, the staff would recommend assessing additional threat and vulnerability information to support developing the ISFSI-specific regulatory guidance document. Staff would provide the results of the threat and vulnerability evaluation, and any recommendations, to the Commission for its review. The staff resources necessary to complete such an evaluation are discussed in the Resources section of the main Commission paper.

Background Information on Threat Assessments and CARVER Analysis

Summary

This enclosure presents supplementary background information to assist the Commission in evaluating the options set forth for the various policy issues. Specifically, the staff is providing information on differences between a threat-based approach and a risk-based (i.e., vulnerability-informed) approach to develop security regulations. Additionally, the staff is also providing information on how elements of a CARVER[1] analysis could be applied to independent spent fuel storage installation (ISFSI) security by licensees as part of a vulnerability-based approach.

Design Basis Threat Approach versus Vulnerability Analysis Approach

There are two basic methods that can be used by staff in designing physical security system requirements to protect NRC-regulated assets against malevolent acts. One method, used by the NRC, is to develop a design basis threat (DBT) that is based on actual terrorist and criminal activity. A threat assessment is conducted by staff from the Office of Nuclear Security and Incident Response, Division of Security Operations, who examine the domestic and international terrorist and criminal interests in the NRC-regulated asset (e.g., a licensed facility or radioactive/nuclear material) and examine the training, techniques, procedures and equipment used and discussed by these groups. The staff further analyzes these various attributes through the use of additional screening criteria [redacted] to define a final DBT picture. This threat based approach is not considered a worst case or all encompassing threat, but has a narrower threat picture that defines the type of threat characteristics the NRC considers most likely to be seen and that a private guard force would be required to defend against. This type of methodology is used to develop and inform performance-based security requirements and is used for the highest risk NRC-regulated assets.

A second method is to conduct a vulnerability analysis using a methodology such as the CARVER analysis (see below). The CARVER analysis methodology includes threat assessment information that identifies weaponry, tactics, and techniques that could be used by terrorist and criminal groups. This is the same threat assessment information as is used at the beginning of the DBT methodology. The vulnerability portion of the CARVER analysis is then conducted to evaluate whether anything in the threat assessment could significantly damage the asset and its surrounding environs. The results of the damage assessment are used to identify preventive or mitigative features that are then factored into the design of the physical security system. While this method also contains a threat component, its scope is more

[1] C.A.R.V.E.R. analysis includes an evaluation against the following factors: Criticality - identify critical assets; Accessability - determine ease of access to critical assets; Recuperability - compare time to repair, replace, or bypass critical assets; Vulnerability - evaluate security system effectiveness against malevolent capabilities; Effect - consider the scope and consequences of the adverse effects from malevolent acts; and Recognizability - evaluate the potential that adversaries would recognize a critical asset.

encompassing than a DBT and it can be bounded by policy decisions. Consequently, the use of CARVER methodology may be more appropriate for lower risk assets (e.g., those assets that do not require force-on-force level of security performance evaluation).

CARVER Analysis Methodology

The regulatory structure proposed in Option 3 of Policy Issue 3 (see Enclosure 3)[2] would nominally be in the form of a CARVER analysis. Figure 5-1 depicts a CARVER analysis model that could be applied to ISFSI security issues.

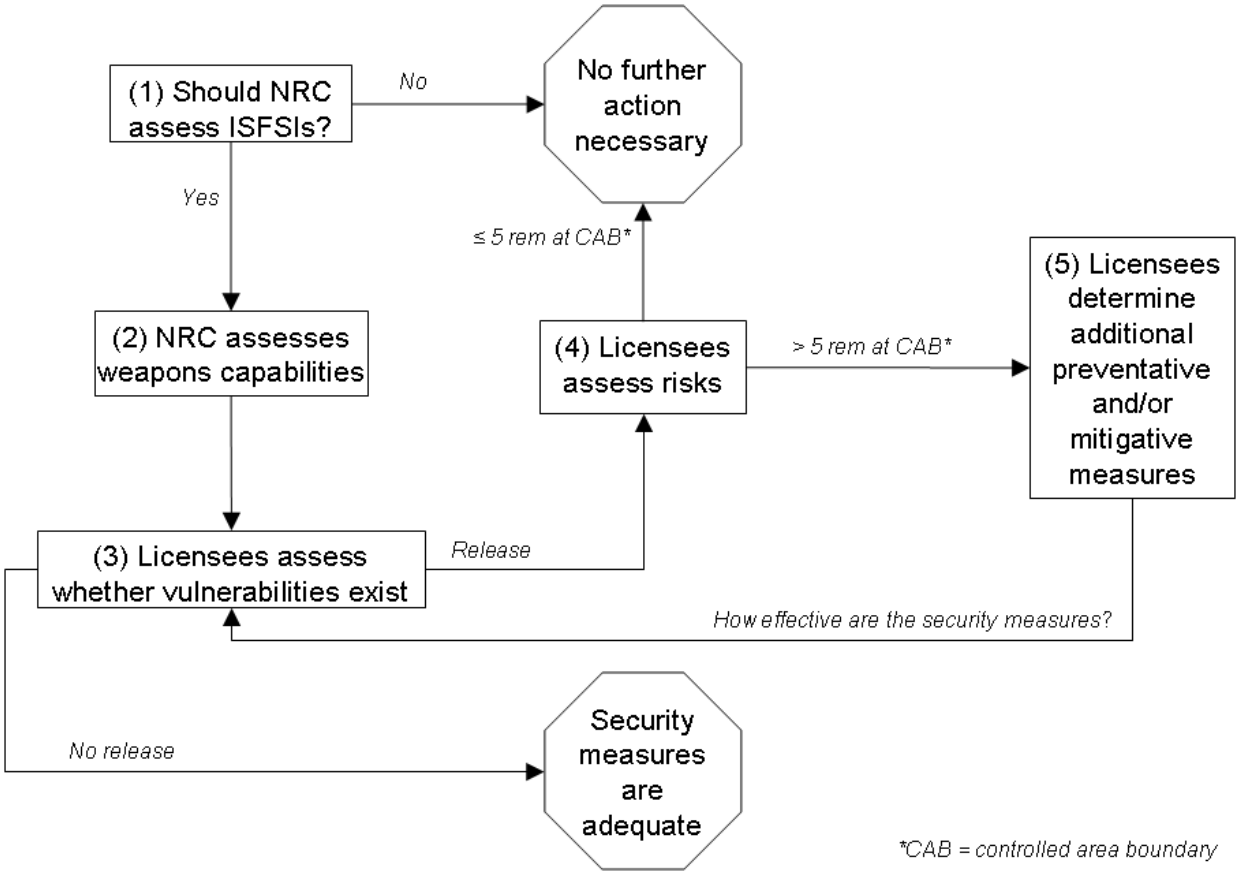

Figure 5-1. CARVER Analysis as Applied to ISFSI Security Issues

A CARVER analysis is an analytical methodology that is used to evaluate the risk (or vulnerability) to critical assets. This methodology has been successfully used by security

[2] Enclosure 3, "Should the Design-Basis Threat for Radiological Sabotage Be Applied Consistently to All Independent Spent Fuel Storage Installations (Not Just to General Licensees)? (Policy Issue 3)."

professionals in various industries (e.g., oil and petrochemical) and the U.S. government (e.g., the Departments of Defense, State, and Homeland Security) since 1970 to assess vulnerabilities and risks, and to evaluate mitigative or compensatory measures. Because the CARVER analysis methodology has been in use by security professionals in various industries and the U.S. government for this length of time, a significant body of expertise in these analyses would exist for ISFSI licensees to draw upon [in accomplishing such an analysis].

As indicated in Figure 5-1 above, completion of a CARVER analysis for an ISFSI would require actions by both the NRC and the licensee. The NRC and licensee would be responsible for different portions of a CARVER analysis. These activities are described below and are indicated in Figure 5-1 above. (Note: As an aid to the reader, the staff has added identification numbers to the boxes in Figure 5-1 which correspond to the text below.)

The NRC would:

> (1) Develop regulations identifying that ISFSIs are an asset that requires protection to ensure that public health and safety and common defense and security are adequately protected, and requiring licensees to complete an analysis to provide high assurance that the ISFSIs physical protection system provides this adequate protection; and
>
> (2) Develop regulatory guidance to characterize the weapons capabilities or weapons effects (i.e., the phenomena created by certain weaponry—either manufactured or improvised) for which ISFSI vulnerabilities may exist and which would be used by a licensee in their analysis.

The licensee would:

> (3) Evaluate whether the weapons effects specified in the regulatory guidance would create a vulnerability for their facility (i.e., a possible breach of a storage cask's confinement boundary); and
>
> (4) If so, evaluate whether the release of radioactive material from a storage cask in their facility could result in a potential dose to a maximally exposed individual at the controlled area boundary exceeding the 0.05-Sv (5-rem) dose limit;[3] [4] and

[3] The dose criteria in Title 10 of the *Code of Federal Regulations* 72.106, "Controlled area of an ISFSI or MRS," (0.05 Sievert (Sv) [5 rem] total effective dose equivalent; 0.15 Sv [15 rem] to the lens of the eye; 0.5 Sv [50 rem] as either the sum of the deep dose equivalent and any organ dose, or the shallow dose equivalent to the skin or any extremity) are hereinafter referred to as the 0.05-Sv (5-rem) dose limit.

[4] As discussed in Policy Issue 2, the staff would recommend a 0.05-Sv (5-rem) dose limit at the controlled area boundary and an additional verification of a 0.01-Sv (1-rem) dose limit at the site area boundary; hereinafter, called the 0.05-Sv (5-rem) dose limit.

(5) If so, identify changes to the design or operation of the ISFSI, changes to the protective strategy, or the employment of natural or engineered security features that would either prevent the vulnerability or allow the licensee to mitigate the effects of a release to achieve a potential dose to an individual at the controlled area boundary less than the 0.05-Sv (5-rem) dose limit.

The licensee would repeat steps (3), (4), and (5), as required, to verify that it can meet the 0.05-Sv (5-rem) regulatory dose limit. The licensee would then revise and update their physical security plans to reflect any necessary changes to their physical protection system or protective strategy to accomplish this objective.