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.