Staff's Response to Alternate View

A staff member in the Office of Nuclear Security and Incident Response (NSIR) provided an alternate view recommending an additional option for Commission consideration. The additional option is an alternative technical approach for the rulemaking, under which the staff would codify the security orders issued after September 11, 2001 (post-9/11 security orders) for independent spent fuel storage installations (ISFSIs), apply the design-basis threat (DBT) for radiological sabotage to all ISFSIs, and remove the 0.05-sievert (5 rem) dose criterion from Title 10 of the *Code of Federal Regulations* (10 CFR) 73.51, "Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste." The NSIR management and staff appreciate the raising of the alternate view but have not incorporated it into this paper. Additionally, the alternate view does not change the staff's recommendation.

The paper presents four options for Commission consideration and recommends Option 1 (to discontinue the rulemaking). The additional option in the alternate view is described as a combination of Option 2 (codify the post-9/11 security orders) and elements of Option 4 (to perform a future reassessment of alternative technical approaches for the rulemaking). Specifically, the additional option is an alternative technical approach for the ISFSI security rulemaking that includes the following elements:

(1) Remove the current 0.05-sievert (5 rem) dose criterion from 10 CFR 73.51 in all circumstances.

(2) Apply to specific-license ISFSIs the DBT for radiological sabotage that is currently applicable to general-license ISFSIs.

(3) Codify the post-9/11 security orders.

The alternate view provides a basis for incorporating each of these elements into the alternative technical approach, along with a basis for the general premise that this approach is the only technically viable option for prompt rulemaking without a substantive reassessment. The staff addresses these three elements and the question of technical viability below.

Element 1: Remove Existing Dose Criterion

Summary of the Alternate View's Basis

- The absence of a technically viable release fraction methodology is a foundational barrier to establishing a regulatory process that requires a licensee or the staff to determine whether a specific-license ISFSI's physical security program meets the 0.05-sievert (5 rem) dose limit of 10 CFR 73.51.

- The staff's evaluation of the nonviability of the release fraction methodology serves as an impediment to a rulemaking that would continue the current 0.05-sievert (5 rem) dose limit in the current acceptance criterion in 10 CFR 73.51.

Staff's Response

The staff does not agree that the difficulty of developing a viable release-fraction methodology for the dose-based approach poses a barrier to establishing a methodology requiring licensees or the staff to determine whether an ISFSI's physical security program meets the 0.05-sievert

(5 rem) dose limit of 10 CFR 73.51. If the staff were to continue to pursue a rulemaking to require licensees to demonstrate that they could meet a dose limit, there are alternative methodologies it could assess that do not require the use of dose assessments based on release fractions resulting from specific security scenarios, as envisioned under the dose-based approach.

The staff does not agree that the nonviability of the release fraction methodology is an impediment to maintaining the current 0.05-sievert (5 rem) dose criterion language in 10 CFR 73.51. Within the current regulatory framework, the 0.05-sievert (5 rem) safety-related dose criterion exists as a bounding criterion because specific-license ISFSIs implement security measures to prevent loss of control of the facility. The challenges with establishing a new release-fraction methodology resulting from specific security scenarios to implement the proposed dose-based approach have no bearing on maintaining the existing regulatory framework for ISFSI security.

Element 2: Apply the DBT to All ISFSIs

Summary of the Alternate View's Basis

- In Enclosure 3 of SECY-07-0148, "Independent Spent Fuel Storage Installation Security Requirements for Radiological Sabotage," dated August 28, 2007, the staff concluded that both the dose-based approach and the DBT-based approach (i.e., the option of consistently applying the DBT for radiological sabotage to both general- and specific-license ISFSIs), along with developing an ISFSI-specific adversary characteristics document, were "technically acceptable, and either option would result in an appropriate level of security for ISFSIs."

- Feedback from cleared nongovernmental organization (NGO) personnel supported the use of a DBT-based approach in an ISFSI security rulemaking.

Staff's Response

As with the dose-based approach, under the DBT-based approach described in SECY-07-0148, licensees would be required to design their protective strategies based on the results of a dose assessment to meet a 0.05-sievert (5 rem) dose criterion.[1] The difference between the two

[1] SECY-07-0148, Enclosure 3, states the following:

> 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.

approaches is that the DBT-based approach requires ISFSI licensees to design their protective strategies to protect against the DBT (i.e., it is threat based), while the dose-based approach requires ISFSI licensees to design their protective strategies to protect against the specific security scenarios that the staff would develop (i.e., it is vulnerability based). However, both approaches were developed to be "performance based" by requiring the protective strategy to be designed based on the results of a dose assessment. In SECY-07-0148, the staff stated that "[t]he 'performance based' element would apply specific radiological dose acceptance limits to ISFSI security activities."

The alternative technical approach presented in the alternate view would not apply the DBT in combination with requiring a dose assessment to demonstrate that the dose criterion would be met. Instead, it would apply the DBT while eliminating the dose criterion. Given this difference, the staff does not agree with the implication in the alternate view that the staff's finding, in SECY-07-0148, Enclosure 3, that the DBT-based approach is "technically acceptable" and "would result in an appropriate level of security for ISFSIs" applies to the technical approach presented in the alternate view.

Similarly, the supportive feedback the staff received from NGO personnel on the DBT-based approach does not indicate that the NGO personnel would support the technical approach presented in the alternate view. The NGO personnel indicated a preference for a DBT-based approach in which licensees would design their protective strategies based not on their ability to limit the dose consequences of a security event, but on their ability to prevent the event from occurring. In other words, the NGO personnel preferred the protective strategy that the staff described in SECY-07-0148, Enclosure 3, as a "denial-of-task" protective strategy. As with the dose-based approach, if licensees could not demonstrate that they could meet the 0.05-sievert (5 rem) dose criterion, they could be required to implement this denial-of-task protective strategy instead of the current "detect, assess, and communicate" strategy.[2] In contrast, the technical approach proposed in the alternate view would apply the DBT but would not require a dose assessment to confirm that a dose limit would be met, nor would it require a denial-of-task protective strategy. During the public meeting conducted as part of the development of this paper, an NGO stakeholder reiterated a preference for a rulemaking that would require licensees to implement a denial-of-task protective strategy. Additionally, in Enclosure 2 of SECY-10-0114, "Recommendation to Extend the Proposed Rulemaking on Security Requirements for Facilities Storing Spent Nuclear Fuel and High-Level Radioactive Waste," dated August 26, 2010, the staff stated the following about stakeholder engagement on a technical approach that would apply the DBT without requiring a dose assessment:

> The staff would address stakeholders' comments to use the DBT approach by explaining that the licensees would likely be required to implement a denial protective strategy for all ISFSIs and MRSs [monitored retrievable storage installations] if a dose calculation were not required to assess the impact of potential releases at a licensee's specific site.

---

[2] SECY-07-0148, Enclosure 3, states the following:

> Regardless of which option 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. No ISFSI licensees currently implement a "denial of task" protective strategy.

Element 3: Codify the Post-9/11 Security Orders

Summary of the Alternate View's Basis

The paper does not sufficiently consider the longer-term qualitative costs and benefits that would arise from increased openness and transparency and increased opportunity for public comment.

Staff's Response

The staff evaluated the costs and benefits of codifying the security orders and the alternate view does not provide new or different quantitative or qualitative factors that were not considered in the staff's evaluation. The paper does address benefits of codifying the orders. In the description of Option 2, Enclosure 1 to the paper states that codifying the post-9/11 security orders would "provide an opportunity for public comment and engagement and would provide some qualitative benefits such as openness and transparency for future applicants and the public." Therefore, the overall conclusion for Option 2, that the significant costs of a rulemaking would not be warranted is not changed by the information provided in the alternate view.

Element 4: Viability of the Alternative Technical Approach for Prompt Rulemaking

Summary of the Alternate View's Basis

- A DBT-based rulemaking approach is the only technically viable option remaining if the Commission desires to proceed promptly to rulemaking.

- Codifying the current orders and applying the DBT for radiological sabotage under 10 CFR 73.51 provides an improvement in the effectiveness of security.

- The Commission's previous detailed consideration of the DBT-based approach in SECY-07-0148 and the information in the current paper obviate the need for a substantive reassessment, given the nonviability of a release fraction methodology.

Staff's Response

The current regulatory framework, including the additional requirements in the post-9/11 security orders, provides reasonable assurance of adequate protection of public health and safety for ISFSIs. The staff does not find any additional information in the alternate view that would warrant proceeding promptly to rulemaking.

In Staff Requirements Memorandum (SRM)-SECY-07-0148, dated December 18, 2007 (ML073530119), the Commission approved the staff's recommendation to pursue a rulemaking to "develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements" using the dose-based approach. As described above, the performance-based element of the dose-based approach comes from the application of "specific radiological dose acceptance limits to ISFSI security activities." The alternate view does not address how the alternative approach, which eliminates the performance-based element of a dose criterion, would support the staff's development of risk-informed and performance-based security requirements, as directed by the Commission in SRM-SECY-07-0148.

The staff does not agree that the alternate view adequately demonstrates that the alternative technical approach provides an improvement to the effectiveness of security. The alternate view does not evaluate the impacts from changing the current regulatory framework by removal of the dose criterion, which has been in the regulations since 1998 and is implemented by all current ISFSI-specific licensees. The alternate view states that the Commission's previous detailed consideration of the DBT-based approach in SECY-07-0148 obviates the need for a substantive reassessment. However, the alternate view does not discuss the staff's assessment, in Enclosure 1 of SECY-07-0148, of the impacts to the effectiveness of security that could result from eliminating the dose criterion. In this assessment, the staff presented the following disadvantages of eliminating the dose criterion:

- It would appear to reduce the security requirements for noncollocated specific licensees, which could negatively impact public confidence.

- 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.

The staff does not agree that the alternate view demonstrates that the alternative technical approach is the only technically viable approach that would support a rulemaking, as directed in SRM-SECY-07-0148, to develop "new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements." The alternate view does not consider the alternative technical approaches that could come from a fulsome reassessment, as described under Option 4, such as applying the DBT and maintaining the current dose criterion, increasing the dose limit, or requiring a denial-of-task strategy, all of which could potentially be technically viable.

Conclusion

Given the staff's concerns regarding the viability of the dose-based approach, the paper includes Option 4, under which the staff would perform a future reassessment to identify alternatives to the dose-based approach. The description of Option 4 in the paper presents the elimination of the dose criterion and the application of the DBT to all ISFSIs as two of several approaches that the staff had previously considered and could consider during a reassessment. The paper states that any rulemaking options that could result from the reassessment could include codification of the post-9/11 security orders. The alternate view provides an option for rulemaking that would combine these three elements, and the alternate view recommends that the Commission approve this option on the basis that it is the only remaining viable option for prompt rulemaking.

As discussed above, the staff does not agree that the alternate view has demonstrated that an approach to apply the DBT and eliminate the dose criterion is the only remaining technically viable option for a rulemaking to "develop new, risk-informed, performance-based security requirements applicable to all ISFSI licensees to enhance existing security requirements." The staff does not agree that the alternate view has established the viability of this technical approach nor the nonviability of other alternative approaches. The staff also does not find that the alternate view provides information that would warrant proceeding promptly to rulemaking. The current regulatory framework, including the additional requirements in the post-9/11 security orders, provides reasonable assurance of adequate protection of public health and safety for ISFSIs. The alternate view does not change the staff's recommendation of Option 1, to discontinue the rulemaking.