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.

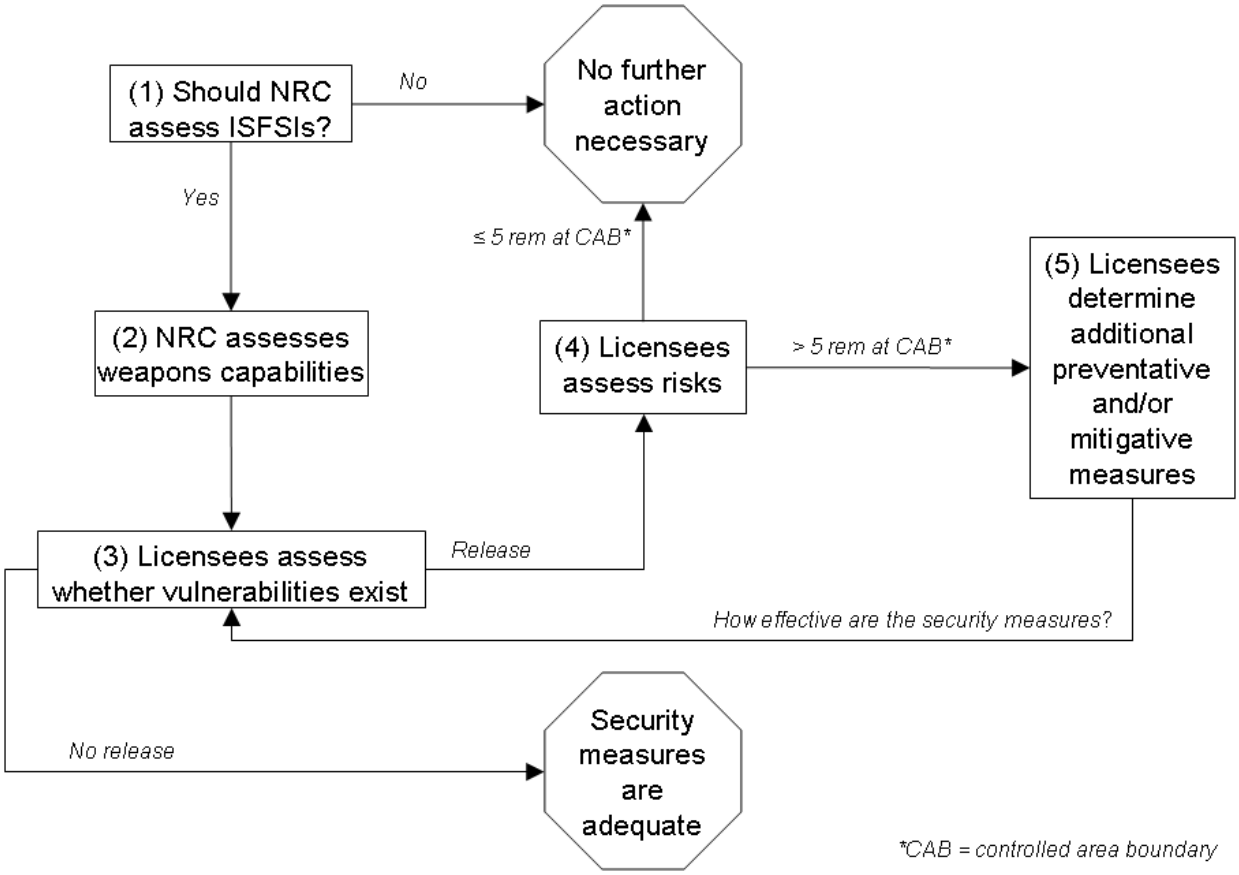

Figure 5-1. CARVER Analysis as Applied to ISFSI Security Issues

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.