Regulatory Analysis of Final Rule
10 CFR Part 73.1- Design Basis Threat

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation

September 2006

Executive Summary

The design basis threat (DBT) requirements in 10 CFR 73.1(a) describe general adversary characteristics that designated licensees must defend against with high assurance. The Nuclear Regulatory Commission (NRC) requirements include protection against radiological sabotage (applied to power reactors and Category I fuel cycle facilities) and theft or diversion of NRC-licensed strategic special nuclear material (SSNM) (applied to Category I fuel cycle facilities). The DBTs are used by these licensees to form the basis for site-specific defensive strategies.

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security to ensure that nuclear facilities continued to have effective security measures in place for the changing threat environment, and concluded that some elements of the DBTs required enhancement. After soliciting and receiving comments from Federal, State, and local agencies, and industry stakeholders, the NRC imposed by order supplemental DBT requirements that contained additional adversary characteristics. The April 29, 2003 DBT Orders required nuclear power reactors and Category I fuel cycle licensees to revise their physical security plans, security personnel training and qualification plans, and safeguards contingency plans to defend against the supplemental DBT requirements.

This regulatory analysis considers only one alternative for addressing changes to the DBT requirements. As required by the EPAct, the Commission is obligated to implement regulations revising the DBT. Nonetheless, the "no action" alternative is included in this analysis to provide a baseline for determining the costs and benefits of the DBT rulemaking. Because the DBT involves the discussion of information that includes safeguards information or classified information, the NRC evaluated three rulemaking strategies for the most appropriate approach.

On November 7, 2005, the Commission published a proposed rule (70 FR 67380) for public comment to make generically applicable the security requirements previously imposed by the Commission's April 29, 2003 Orders, which applied to existing licensees. The proposed rulemaking took into consideration the 12 factors specified in the Energy Policy Act (EPAct) of 2005, as well the petition for rulemaking (PRM) filed by the Committee to Bridge the Gap (PRM-73-12) on July 23, 2004.

The Commission has received and evaluated public comments that are reflected in the final rule. In all, 919 comments were received. Sources for these include about nine hundred individuals, one county, thirteen public interest groups, one utility involved in nuclear activities, and two nuclear industry groups. The comments covered a range of issues, some of which are beyond the scope of this rulemaking in that they are specific to protective measures but did not relate to the adversary characteristics. There was one comment on the regulatory analysis document questioning the adequacy of the analysis. Response to this question is provided in Section II of the *Federal Register* Notice.

Based on the staff's evaluation of public comments and further consideration of factor two of the EPact, the final rule text has been revised to explicitly include the cyber threat. The NRC staff liaison with U.S. Intelligence and Law Enforcement Communities indicates that the cyber threat is an enduring one, and likely will increase in capability and frequency in the future. In

light of this threat, comments on the proposed rule as well as the cyber security programs already initiated by the industry, the staff decided to use the current 10 CFR § 73.1 rulemaking process to initiate the inclusion of formal cyber threat language in the DBTs.

Table of Contents

I. Statement of Problem and NRC Objectives

(a) History and Background

The DBT requirements in 10 CFR 73.1 describe general adversary characteristics that designated licensees must defend against with high assurance. These NRC requirements include protection against radiological sabotage (generally applied to power reactors and Category I fuel cycle facilities) and theft or diversion of NRC-licensed SSNM (generally applied to Category I fuel cycle facilities). On November 7, 2005 (70 FR 67380), the Commission published a proposed rule for public comment seeking to amend its regulation that governs the requirements pertaining to the DBTs. The DBTs are used by licensees to form the basis for site-specific defensive strategies implemented through physical security plans, safeguards contingency plans, and security personnel training and qualifications plans. Amendment of the DBT rule was influenced by a number of factors described below.

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place for the changing threat environment. In so doing, the NRC recognized that some elements of the DBTs required enhancement due to the escalation of the domestic threat level. After soliciting and receiving comments from Federal, State, local agencies, and industry stakeholders, the NRC imposed by orders supplemental DBT requirements which contained additional detailed adversary characteristics. The NRC considered the balance between licensee responsibilities and the responsibilities of the local, State and Federal Governments during the development of the April 29, 2003 DBT Orders.

The April 29, 2003 DBT Orders required nuclear power reactors and Category I fuel cycle licensees to revise their physical security plans, security personnel training and qualification plans, and safeguards contingency plans to defend against the supplemental DBT requirements. The Orders resulted in licensee security enhancements such as increased patrols; augmented security forces and capabilities; additional security posts; additional physical barriers; vehicle checks at greater standoff distances; better coordination with law enforcement and military authorities; augmented security and emergency response training, equipment, and communication; and more restrictive site access controls for personnel, including expanded, expedited, and more thorough worker initial and follow-on screening. Currently, all power reactor and Category I fuel facilities have received NRC approval of security plans consistent with the DBTs imposed by the April 2003 Orders.

On November 7, 2005 (70 FR 67380), the Commission published for public comment the proposed 10 CFR 73.1 rule that would amend the Commission's regulations to make generically applicable the security requirements previously imposed by the Commission's April 29, 2003 DBT Orders, which applied to existing licensees, and redefines the level of security requirements necessary to ensure that the public health and safety and common defense are adequately protected.

(b) Objective of Final Rulemaking

The final rulemaking makes generically applicable the supplemental requirements put in place by the Orders and revised the existing DBT requirements in § 73.1(a) and satisfies the Commission's statutory obligation under section 651 of the EPAct to initiate and complete a rulemaking revising the DBT. The final rule describes the DBTs at a level of detail comparable

to the current rule. Specific details related to the threat, which include both safeguards information and classified information, are consolidated in adversary characteristics documents that include requirements consistent with those in the DBT orders. The adversary characteristics documents (ACDs) are available to those with authorized access. The final rule includes the DBTs for both radiological sabotage (applied to power reactors and Category 1 fuel cycle facilities) and theft and diversion (Category 1 fuel cycle facilities). The final rulemaking provides the Commission's consideration of the 12 factors specified in the EPAct, the petition for rulemaking filed by the Committee to Bridge the Gap (PRM-73-12), and public comments on the proposed rule.

In all, 919 comments were received on the proposed rulemaking from the public, industry groups and public bodies. The comments covered a range of issues, some of which are beyond the scope of this rulemaking in that they are specific to protective measures but did not relate to the adversary characteristics. The final rule is reflective of the Commission's consideration and deliberation on all these comments.

(c) Backfit Rule Considerations

The NRC has determined, pursuant to the exception in 10 CFR 50.109(a)(4)(iii) and 10 CFR 70.76(a)(4)(iv), that a backfit analysis is unnecessary for this final rule. Section 50.109 and § 70.76(a)(4)(iv) state, in pertinent part, that a backfit analysis is not required if the Commission finds and declares with appropriate documented evaluation for its finding that a "regulatory action involves defining or redefining what level of protection to the public health and safety or common defense and security should be regarded as adequate." The final rule increases the security requirements currently prescribed in NRC regulations, and is necessary to protect nuclear facilities against potential terrorists. When the Commission imposed security enhancements by order in April 2003, it did so in response to an escalated domestic threat level. Since that time, the Commission has continued to monitor intelligence reports regarding plausible threats from terrorists currently facing the U.S. The Commission has also gained experience from implementing the order requirements and reviewing revised licensee security plans. The Commission has considered all of this information and finds that security requirements similar to those previously imposed by the DBT orders, which applied only to existing licensees, should be made generically applicable. The Commission further finds that the final rule would redefine the security requirements stated in existing NRC regulations, and is necessary to ensure that the public health and safety and common defense and security are adequately protected in the current, post-September 11, 2001 environment.

II. Analysis of Alternatives

There is only one alternative for addressing changes to the DBT requirements. As required by the EPAct, the Commission is obligated to implement regulations revising the DBT. Nonetheless, the "no action" alternative is included in this analysis to provide a baseline for determining the costs and benefits of the DBT rulemaking.

(a) No Action Alternative

This alternative is included to serve as a baseline, against which the DBT requirements can be measured. As discussed above, the Commission is required by the EPAct to conduct a rulemaking to revise the DBT.

(b) Rulemaking Alternatives

The second alternative is to revise § 73.1(a) DBT requirements. There are several different strategies for revising the requirements in the regulations. The strategies are:

(1) A rulemaking would contain the DBT details (which are safeguards and classified information) but which would withhold this information from public disclosure. This would require a change to Part 2 to develop a new rulemaking process.

(2) A rulemaking that would remove all detail from the regulation but refer to documents that contain the DBT details.

(3) A rulemaking that would revise § 73.1(a) requirements to remove detail that might provide useful information to potential adversaries and follow an approach similar to the current regulation by not referencing a document containing DBT attributes, but keeping the level of detail in the rule language consistent with the current detail level in an effort to maximize the opportunity for meaningful stakeholder participation.

The first strategy would require an amendment to 10 CFR Part 2 to develop the new rulemaking procedures that would account for the withholding of safeguards and classified information from the public. This approach envisions neither public notice of a rulemaking nor an opportunity for the public to comment on the proposed DBT regulation. This proposed rule could contain detailed DBT requirements (which are safeguards and classified information), but the DBT detail would be withheld from the public. Developing new rulemaking procedures would likely involve considerable resources and there is the potential that this process would not comply with the Administrative Procedure Act (APA). Given these challenges and the additional expenditure of staff resources to pursue this approach, this strategy was not chosen.

The second strategy would remove all DBT details from § 73.1(a) but incorporate by reference safeguards or classified documents containing the DBT requirements. This option would limit availability of information that could aid potential adversaries. However, removing all the DBT details to a document that would be restricted from public access (due to the safeguards and classified content), would unduly limit other DBT details which are meaningful for the public to comment on but are not useful to potential adversaries in planning or carrying out attacks. This approach would also create questions regarding whether the approach provides the public with a meaningful opportunity to comment. For this reason, this approach was not selected.

The third strategy would revise the § 73.1(a) requirements to accurately reflect the new DBT requirements except for information that could be useful to potential adversaries, while removing information that is outdated. This strategy would not require reference to a document outside of the regulations, and in this sense, this strategy is similar to current regulatory practice (i.e., § 73.1 has been structured this way since its inception). This approach would maintain a level of detail in the rule text that is comparable to the current § 73.1 in an effort to maximize the opportunity for external stakeholders to participate in the rulemaking. Compared to the other rulemaking strategies described above, this rulemaking strategy would provide the public with the greatest opportunity to comment and participate in the rulemaking process. However, the public's participation and access to safeguards and classified information is restricted to members of the public who have authorized access. This is the rulemaking strategy that best balances meaningful public participation with the need to protect safeguards and classified sensitive information. As such, this strategy would warrant the expenditure of

agency resources**;** consequently, the NRC selected this approach.

III. Estimate and Evaluation of Values and Impacts

(a) Overview

This final rule revises the governing regulations pertaining to the DBT, to make generically applicable security requirements similar to those previously imposed by the Commission's April 29, 2003 Orders which applied to existing licensees, and redefines the level of security requirements necessary to ensure that the public health and safety and common defense and security are adequately protected.

This rule has no impact on facility risk. This rule does not change the risk associated with security-related events from the current level because requirements that are currently in place per the Orders, remain in place. Because there will be no net change in risk related to radiological sabotage or theft and diversion (the implemented Orders have already addressed this), there will be no net change in potential value (in terms of reduced risk) due to this rulemaking.

This rulemaking adds value, because revising § 73.1(a) requirements to more accurately reflect the implemented DBT requirements (with the constraint that certain information would not be revealed within § 73.1(a)), increases the regulatory coherency.

(b) Impacts on Licensees

Impacts upon the licensees from this final rule will be minimal. Because the adversary characteristics will remain consistent with those promulgated by Orders and ICM, no technical changes will be required. The NRC has previously reviewed and approved the changes required to meet the Orders. Licensees may need to update references in their security plan documentation in order to meet rule changes which could be accomplished in accordance with § 50.54(p) or § 70.32(e), as applicable, without NRC review and in conjunction with future plan updates. The staff does not anticipate the need to review revisions to security plans solely to implement the revisions of the § 73.1 rule. However, future changes in the threat environment may affect the ACDs, and could possibly affect the licensees' security plans requiring either NRC's approval or official communications noting the changes to the NRC. This may also impose additional burden to the licensees. No attempt has been made to quantify the potential speculative changes in the ACDs.

(c) Impacts on the NRC

a. The primary impact on the NRC has been the resources expended in conducting this rulemaking, including the consolidation of security guidance related to the DBTs. This guidance was developed during the post September 11, 2001, time frame, and was used by licensees to revise security plans per the new DBT. The effort associated with this rulemaking is to consolidate the DBT guidance into stand-alone documents, not to revise or create the guidance.

b. NRC would not need to expend resources to review and approve security plans as a result of the revised DBTs because this effort has already occurred and was

completed on October 29, 2004.

c. There would be no additional resource impacts from adjusting inspection guidance or processes to take into account the existence of the new DBT requirements that have not already been incurred as a result of the April 29, 2003 DBT Orders implementation. The NRC uses force-on-force exercises as a primary means to judge the effectiveness of security plans. The force-on-force exercises were revised concurrent with the DBT Order implementation effort, and as such, this impact is not part of this rulemaking.

(d) Impacts on Other Stakeholders

The NRC staff has not identified any impacts upon other stakeholders. Public health and safety and common defense and security would continue to be adequately protected through either the existing requirements implemented by Orders or the revised requirements (which more closely align the governing regulations with the orders). There would be no new costs to other stakeholders of implementation associated with the rulemaking.

(e) Values of the Final Rulemaking for NRC, Industry, and Other Stakeholders

The NRC staff has identified a value to stakeholders, in that this process allowed public participation in the rulemaking. In terms of values measured by risk reductions, the requirements are not changing and as a result, this rulemaking does not impact the risk associated with security events. Further, regulatory efficiency is attained by making generically applicable the supplemental requirements put in place by the Orders and the existing DBT requirements in § 73.1(a).

IV. Decision Rationale for Selection of Final Action

This regulatory analysis is largely qualitative which is dictated by the nature of this rulemaking that seeks to more closely align § 73.1(a) with the requirements already imposed through Orders. Even though the final rule includes a cyber attack as an element of the rule, this element was implicitly addressed in the proposed rule, and it does not require licensees to take action or respond to the revised requirement, since the affected licensees have been directed through ICM EA-02-026 to consider and address cyber safety and security vulnerabilities. In April 2003, the revised DBT Orders (EA-03-086) and (EA-03-087) contained language concerning the cyber threat. Licensees were subsequently provided with a cyber security self-assessment methodology, and additional guidance issued by the Nuclear Energy Institute (NEI), in order to facilitate development of site-specific cyber security programs. The designated licensees have done so accordingly.

It should be noted that in the proposed § 73.55 rulemaking, the NRC is proposing further requirements for mitigating the cyber threat. The regulatory impact of those requirements will be contained in the regulatory analysis for the § 73.55 rulemaking and are independent of this action.

Implementation

NRC is amending § 73.1(a) to consolidate and more closely align NRC regulations with the supplemental DBT requirements required by April 29, 2003 Orders. The final rule does not

impact licensees nor does the final rule require licensee responses, submittals, or affirmative actions. Review guidance was developed during the order implementation period; this rulemaking does not change that guidance, but consolidates requirements where appropriate. The final rule will be publicly noticed and will be effective 30 days after publication of the rule. No impediments to implementation of the recommended alternative have been identified.