September 29, 2006

MEMORANDUM TO : Michael J. Case, Director, ADRA, NRR
R. Rasmussen, NSIR, SRB
L. Solander, NSIR, PMDA
D. Dorman, NSIR, DSO
V. Ordaz, NSIR, DSP
G. Tracy, Director, NSIR, DSP
R. Way, NSIR, DSO
Jack R. Strosnider, Director, NMSS
C. Miller, Directror, NMSS
Roy P. Zimmerman, Director, NSIR
Brian W. Sheron, Director, RES
Cynthia A. Carpenter, Director, OE
Stuart A. Treby, OGC
Michael T. Lesar, Chief, RDB, ADM

FROM: Ho Nieh, Acting Director ***/RA/***
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

SUBJECT: FINAL RULE: DESIGN BASIS THREAT (DBT) 10 CFR 73.1

On November 7, 2005, the NRC published a proposed rule (70 FR 67380) which makes 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 and security are adequately protected. The NRC received 919 comments from the public, stakeholders and local government during the public comment period. The staff has considered and resolved all of the public comments received and made changes to the rule as appropriate. We believe this final rulemaking action will improve the efficiency and effectiveness of the DBT rule.

We are seeking your concurrence on the Commission Paper (ML062130442) and *Federal Register Notice* (ML 062130301), hard copies of which we are transmitting to you separately.

If you have any questions or comments that you would like to discuss, please contact Manash Bagchi (415-2905) or Yong Kim (415-2729) on the rulemaking team.

Please use the blanc form provided in the Enclosure 1 for comments and concurrences. For schedule considerations, please send your concurrences by COB 10 October, 2006.

Enclosures:

1. Form for providing concurrence/comments
2. Rule Package

Enclosure 1

_____
(Date)

MEMORANDUM TO: Ho K. Nieh, Acting Director
Diviion of Policy and Rulemaking
Office of Nuclear Reactor Regulation

FROM : _____

_____

_____

SUBJECT: FINAL RULE: Design Basis Threat (DBT) 10 CFR 73.1

_____ has reviewed the Commission Paper, draft *Federal Register* notice, Regulatory Analysis and Environmental Assessment for the subject final rule in the technical areas under our responsibility and:

☐ I concur with no comments

☐ I concur with the attached changes (see attached markup portions of the Commission Paper and/or the FRN)

☐ I concur with the following comments:

_____

_____

_____

FOR: The Commissioners

FROM: Luis A. Reyes
Executive Director for Operations

SUBJECT: FINAL RULEMAKING TO REVISE 10 CFR 73.1, DESIGN BASIS THREAT (DBT) REQUIREMENTS

PURPOSE:

To obtain Commission approval to publish the final rule for 10 CFR 73.1 and to close Petition PRM-73-12 .

SUMMARY:

The Nuclear Regulatory Commission (NRC) is amending its regulations that govern the requirements pertaining to the design basis threats (DBTs). This final rule makes 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 and security are adequately protected. The final rule will also satisfy the Commission's statutory obligation under Section 651 of the Energy Policy Act of 2005 (EPAct) to initiate and complete a rulemaking revising the DBT, considering the 12 factors specified in the Act. Additionally, a Petition for Rulemaking (PRM-73-12), filed by the Committee to Bridge the Gap, was considered as part of this rulemaking. The NRC partially granted PRM-73-12 in the proposed rule, but deferred action on other aspects of the petition to this rulemaking. The NRC's final disposition of PRM-73-12 is contained in this document.

CONTACTS: Manash Bagchi, NRR/ADRA/PRAB
301-415-2905

Yong Kim, NSIR/DSP/SRB
301-415-2729

BACKGROUND

The 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 (generally applied to power reactors and Category I fuel cycle facilities) and theft or diversion of NRC-licensed Strategic Special Nuclear Material (SSNM) (generally applied to Category I fuel cycle facilities). Radiological sabotage specifically applies to facilities that use special nuclear material. However, current Category I facilities do not typically possess or use nuclear/radioactive materials that could be used to generate a radiological sabotage threat. Possession of these materials would require a licensing action. Theft or diversion applies to facilities that receive, acquire, possess, use, or transfer formula quantities of SSNM. The DBTs are used by these licensees to form the basis for site-specific defensive strategies implemented through security plans, safeguards contingency plans, and security officer training and qualification plans.

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 order supplemental DBT requirements which contained additional detailed adversary characteristics. The Commission 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.

Section 651(a) of the Energy Policy Act of 2005 amended the Atomic Energy Act (AEA) by adding Section 170E, which required the Commission to initiate a rulemaking to revise the DBTs. In addition, Section 170E also directed the Commission to consider in the course of that rulemaking, but not be limited to, 12 factors specified in the statute. The Commission published a proposed rule (See, 70 FR 67380; November 7, 2005) amending its regulation that, among other things, govern the requirements pertaining to the DBTs for public comment. This rulemaking also took into consideration a petition PRM-73-12 filed by the Committee to Bridge the Gap on July 23, 2004.

Summary of Public Comments on Proposed Rule

The proposed rule was published on November 7, 2005, for a 75-day public comment period. A 30-day extension of the comment period was granted to accommodate the shortened comment period caused by the year-end holiday period (71 FR 3791, January 24, 2006). In all, 919 comments were received from the public, stakeholders and local government, out of which approximately 893 comments were form letters. The form letters voiced concerns that the proposed rule did not adequately address the issues raised in PRM-73-12 and the 12 factors of the EPAct, specifically the consideration of water-borne and air-borne threats including requiring licensees to construct “beamhenge” shields to protect against airborne attacks using a large commercial aircraft, and modeling the size of the adversary force on the composition of the September 11th hijackers. The comments have been organized in three groups: (I) Comments regarding the 12 factors of the EPAct, (II) In Scope Comments, raising issues and

questions directly related to the contents of the DBT rule, and (III) Out of Scope Comments, raising issues and questions that are not directly related to the DBT rule, though they are relevant to the security of nuclear facilities. The staff has considered and deliberated on all comments, and provided detailed responses in the attached document.

Changes in Rule Text

After considering the public comments, the 12 factors of the EPAct, and outstanding issues of the PRM-73-12, the staff is proposing to explicitly include cyber as an element of the DBTs. The previous requirements in 10 CFR 73.1 did not have specific adversary characteristics for the threat of a cyber attack. However, the cyber threat was implied as one of the capabilities of the insider.

The staff has several bases for adding the cyber threat element to the final rule. In Section 651(a)(2) of the EPAct, Congress directed the NRC to consider making an "assessment of physical, cyber, biochemical, and other terrorist threats" when writing the revised rule. In addition, the staff had been analyzing the cyber threat well before the EPAct. In February 2002, licensees subject to the DBTs were directed by the Interim Compensatory Measures (ICM) Order (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 the results of pilot studies contracted by NRC, as well as additional guidance issued by the nuclear industry, in order to facilitate development of site cyber security programs. Furthermore, the staff liaison with the U.S. Intelligence and Law Enforcement Communities indicates that the cyber threat is an enduring one, and likely will increase both in capability and frequency in the future. The staff therefore decided to include the cyber threat as an explicit attribute of the DBTs.

The staff concludes that the final revisions to § 73.1 will ensure adequate protection of public health and safety and the common defense and security. The final DBT rule makes generically applicable the DBTs previously imposed by the April 29, 2003 DBT Orders, and used by licensees to develop and implement security measures. The NRC required affected licensees to use the supplemented DBT requirements in the April 29, 2003 Orders to revise their security plans. The staff has reviewed and approved all the affected licensees' security plans, and amended the licenses to ensure that affected licensees fully implement and maintain in effect all provisions of the Commission-approved security plans. Consequently, the final DBTs will not require licensees to revise their current security plans, in spite of the inclusion of the cyber threat as a part of the DBT rule. The change to the rule text is provided in the attached FRN.

Consideration of the 12 factors of the Energy Policy Act of 2005

The EPAct was signed into law on August 8, 2005. Section 651(a) of the EPAct amended the Atomic Energy Act (AEA) by adding Section 170E, which required the Commission to initiate a rulemaking to revise the DBT. In addition, Section 170E

also directed the Commission to consider in the course of that rulemaking, but not be limited to, 12 factors specified in the statute.

The staff considered the 12 factors of the EPAct in conjunction with its experience in the

implementation of the DBT orders, the issues raised in the PRM-73-12, and the public comments on the proposed rule. The staff's conclusions are set forth in the statement of considerations in Section II of the attached FRN.

Resolution of Petition for Rulemaking

The staff incorporated into this rulemaking consideration of a Petition for Rulemaking, filed by the Committee to Bridge the Gap (PRM-73-12) on July 23, 2004. The petition requested that NRC conduct a rulemaking to revise the DBT regulations (including numbers, teams, capabilities, planning, willingness to die and other characteristics of adversaries) to a level that encompasses, with a sufficient margin of safety, the terrorist capabilities demonstrated during the attacks of September 11, 2001. The petition also requested that security plans, systems, inspections, and force-on-force exercises be revised in accordance with the amended DBT. Finally, the petition requested that a requirement be added to Part 73 to require licensees to construct shields against air attack (referred to as "beamhenge") so that nuclear power plants would be able to withstand an air attack from a jumbo jet similar to the September 11, 2001 attacks.

PRM-73-12 was published for public comment in the *Federal Register* on November 8, 2004 (69 FR 64690). There were 845 comments submitted on PRM-73-12, of which 528 were form letters. The staff reviewed both the petition and the comments on the petition against the supplemental DBTs to determine whether the DBTs should be revised as requested by the petitioner. Based on that review, the NRC staff determined that a number of the requested upgrades in PRM-73-12 have already been implemented. However, the staff recommended that the Commission partially grant PRM-73-12 by conducting the proposed rulemaking revising the DBT requirements in § 73.1(a), but deferred action on other requests of the petition, specifically those aspects which deal with air-based attacks, to the final rulemaking.

During the course of this rulemaking, the staff considered whether an airborne threat should be included as part of the DBTs. The staff, after a thorough evaluation and consideration, is proposing that the Commission maintain the two-track response to the air threat that excludes "beamhenges." The staff considered and rejected the "beamhenges" concept. First, the NRC has determined that the active protection against the airborne threat rests with other agencies of the Federal Government including the military. The staff considered that active protection against the airborne threat requires military weapons and ordinances (i.e., ground-based air defense missiles), that rightfully belong to the Department of Defense, and thus the airborne threat is one which is beyond what a private security force can reasonably be expected to defend against. Second, licensees have been directed to implement certain mitigative measures to limit the effects of an aircraft strike. Therefore, the staff proposes denial of the request of the petition PRM-73-12 regarding the inclusion of an airborne threat in the DBT, as well as "beamhenges" as physical security measures.

Contents of the Final Rulemaking Package

This final rulemaking package includes the final rule *Federal Register* notice, which includes the rule language and statement of considerations (Enclosure 1), the supporting regulatory analysis (Enclosure 2), a supporting environmental assessment (Enclosure 3), and a summary of the public comments submitted on the proposed rule (Enclosure 4).

The DBTs reflected in the final rule are supported by the documents identified below, which are either safeguards information or classified, and therefore are withheld from public disclosure and made available only on a need-to-know basis to those with authorized access:

• Radiological Sabotage Adversary Characteristics Document (Safeguards Information)

• Theft or Diversion Adversary Characteristics Document (Confidential)

• Technical Basis Document (Secret)

• Regulatory Guide (RG)-5.69, "Guidance for the Implementation of the Radiological Sabotage Design-Basis Threat" (Safeguards Information)

• RG-5.70, "Guidance for the Implementation of the Theft or Diversion Design-Basis Threat" (Confidential)

Stakeholders, with authorized access, have been informed regarding the content of the regulatory guidance supporting this proposed rule.

| A cyber threat has been included as an explicit attribute of the DBTs in the final rule, which was not included in the proposed rule. However, this does not amend the information collection requirements because it is in alignment with the Interim Compensatory Measures orders (EA-02-026, EA-02-027, EA-02-086, and EA-03-087) and therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C 3501 et seq.).

COORDINATION:

The Office of the General Counsel has no legal objection to this paper.

The Office of the Chief Financial Officer has reviewed this Commission paper for resource implications and has no objections.

The Advisory Committee on Reactor Safeguards (ACRS) elected not to review the final rule requirements.

The Committee to Review Generic Requirements has completed its review of the final rule package and has no objections.

RECOMMENDATIONS:

That the Commission:

1. *Approve* the notice of final rulemaking for publication (Enclosure 1).

2. *Certify* that this rule, if promulgated, will not have a negative economic impact on a substantial number of small entities in order to satisfy the requirements of the Regulatory Flexibility Act, 5 U.S.C. 605(b).3.

3. *Close* the PRM-73-12.

Note:

a. The final rule will be published in the *Federal Register* with a 30-day waiting period prior to its promulgation.

b. The Chief Counsel for Advocacy of the Small Business Administration will be informed of the certification regarding economic impact on small entities and the basis for the certification, as required by the Regulatory Flexibility Act.

c. Copies of the *Federal Register* notice of the proposed rulemaking will be distributed to all affected Commission licensees. The notice will be sent to other interested parties upon request. Copies of the documents are also available in the NRC's Agencywide Documents Access and Management System (ADAMS), the Public Document Room and on the NRC rulemaking Web site.

d. A public announcement will be issued.

e The appropriate Congressional committees will be informed.

Luis A. Reyes
Executive Director
for Operations

Enclosures:
1. *Federal Register* Notice (ML062130301)
2. Regulatory Analysis (ML062130546)
3. Environmental Assessment (ML062130553)
4. Summary of Public Comments on the proposed rule (ML062130575)

RECOMMENDATIONS:

That the Commission:

1. *Approve* the notice of final rulemaking for publication (Enclosure 1).

2. *Certify* that this rule, if promulgated, will not have a negative economic impact on a substantial number of small entities in order to satisfy the requirements of the Regulatory Flexibility Act, 5 U.S.C. 605(b).3.

3. *Close* the PRM-73-12.

Note:

a. The final rule will be published in the *Federal Register* with a 30-day waiting period prior to its promulgation.

b. The Chief Counsel for Advocacy of the Small Business Administration will be informed of the certification regarding economic impact on small entities and the basis for the certification, as required by the Regulatory Flexibility Act.

c. Copies of the *Federal Register* notice of the proposed rulemaking will be distributed to all affected Commission licensees. The notice will be sent to other interested parties upon request. Copies of the documents are also available in the NRC's Agencywide Documents Access and Management System (ADAMS), the Public Document Room and on the NRC rulemaking Web site.

d. A public announcement will be issued.

e The appropriate Congressional committees will be informed.

Luis A. Reyes
Executive Director
for Operations

Enclosures:
1. *Federal Register* Notice (ML062130301)
2. Regulatory Analysis (ML062130546)
3. Environmental Assessment (ML062130553)
4. Summary of Public Comments on the proposed rule (ML062130575)

Adams Package No.: ML062130289 Commission Paper: ML062130442

OFFICE	NRR/PRAB	NSIR/SRB	NRR/PRAB	DPR	NSIR/SRB	NSIR/PMDA	NSIR/DSO
NAME	M.Bagchi	Y.Kim	T. McCune	J. Clifford	R.Rasmussen	LSolander	D. Dorman
DATE	09/14/06	09/14/06	09/29/06	09/29/06	09/30/06		

OFFICE	NSIR/DSP	NSIR/DSP	NSIR/DSO	NRR/DRA	ADM	OCIO	NMSS: D
NAME	V. Ordaz	GTracy	R. Way	Ho Nieh	M. Leasr	BShelton	J. Strosnider
DATE			09/21/06				

OFFICE	RES: D	NSIR: D	NMSS: D	OCFO	OE: D	OGC	NRR: D
NAME	B Sharon	RZimmerman	C. Miller	J. Funches	C.Carpenter	STreby	J. Dyer
DATE							

OFFICE	EDO						
NAME	LReyes						
DATE							

Official Record Copy

[7590-01-P]

NUCLEAR REGULATORY COMMISSION

10 CFR Part 73

RIN 3150-AH60

Design Basis Threat

AGENCY: Nuclear Regulatory Commission.

ACTION: Final rule.

SUMMARY: The Nuclear Regulatory Commission (NRC) is amending its regulations that govern the requirements pertaining to the design basis threats (DBTs). This final rule makes 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 and security are adequately protected. Pursuant to Section 170E of the Atomic Energy Act (AEA), the final rule revises the DBT requirements for radiological sabotage, applicable to power reactors and Category I fuel cycle facilities, and theft or diversion of NRC-licensed Strategic Special Nuclear Material (SSNM), applicable to Category I fuel cycle facilities. Additionally, a Petition for Rulemaking (PRM-73-12), filed by the Committee to Bridge the Gap, was considered as part of this rulemaking. The NRC partially granted PRM-73-12 in the proposed rule, but deferred action on other aspects of the petition to this rulemaking. The NRC's final disposition of PRM-73-12 is contained in this document.

EFFECTIVE DATE: (This rule is effective 30 days after the publication in the *Federal Register*.)

FOR FURTHER INFORMATION CONTACT:

Manash K Bagchi, Office of Nuclear Reactor Regulation, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone (301) 415-2905, e-mail MKB2@NRC.GOV.

SUPPLEMENTARY INFORMATION:

Table of Contents

I. 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, security personnel training and qualifications plans. Amendment of the DBT rule was influenced by a number of factors, which are described below.

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security practices to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place to address with the changing threat environment. As such, the NRC recognized that some elements of the DBTs required a supplement due to the enhanced threat level environment. After soliciting and receiving comments from Federal, State, and local agencies, and industry stakeholders, and an analysis of intelligence information regarding the trends and capabilities of potential adversaries, the NRC imposed supplemental DBT requirements by order on April 29, 2003. The Commission deliberated on the responsibilities of the local, State, and Federal stakeholders to protect the nation and the responsibility of the licensees to protect individual nuclear facilities before issuing the April 29, 2003 DBT Orders.

The April 29, 2003 DBT Orders required nuclear power reactors and Category I fuel cycle facility 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 required licensees to make security

enhancements such as increased patrols; augmented security forces and capabilities; additional security posts and 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 initial and follow-on screening of power reactor and Category I fuel cycle facility employees. After gaining experience with implementation of these Orders, the Commission concluded that the attributes of the Orders should be generically imposed by regulation on certain classes of licensees.

In addition, PRM-73-12 was filed by the Committee to Bridge the Gap on July 23, 2004, and was published for comment. *See*, 69 FR 64690; November 8, 2004. PRM-73-12 requested that the NRC amend its regulations to revise the DBT regulations (in terms of the numbers, teams, capabilities, planning, willingness to die and other characteristics of adversaries) to a level that encompassed, with a sufficient margin of safety, the terrorist capabilities evidenced by the attacks of September 11, 2001. The petition also requested that security plans, systems, inspections, and force-on-force (FOF) exercises be revised in accordance with the amended DBTs, and that a requirement be added to Part 73 to construct shields against air attack (the shields are referred to as "beamhenges") which the petition asserts would enable nuclear power plants to withstand an air attack from a jumbo jet. The NRC partially granted PRM-73-12 in the proposed rule, but deferred action on other aspects of the petition to the final rulemaking. The NRC's final disposition of PRM-73-12 is discussed in Section VI.

Finally, the Energy Policy Act (EPAct) of 2005 was signed into law on August 8, 2005. Section 651(a) of the EPAct amended the AEA by adding Section 170E, which required the Commission to initiate a rulemaking to revise the DBTs. In addition, Section 170E

also directed the Commission to consider in the course of that rulemaking, but not be limited to, 12 factors specified in the statute. As stated in the proposed rule, these factors are:

1. The events of September 11, 2001;
2. An assessment of physical, cyber, biochemical, and other terrorist threats;
3. The potential for attack on facilities by multiple coordinated teams of a large number of individuals;
4. The potential for assistance in an attack from several persons employed at the facility;
5. The potential for suicide attacks;
6. The potential for water-based and air-based threats;
7. The potential use of explosive devices of considerable size and other modern weaponry;
8. The potential for attacks by persons with a sophisticated knowledge of facility operations;
9. The potential for fires, especially fires of long duration;
10. The potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals;
11. The adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility; and
12. The potential for theft or diversion of nuclear material from such facilities.

The Commission took into account a number of issues and sources in conducting this rulemaking, which included its experience in the implementation of the DBT Orders, the issues raised in PRM-73-12, the requirements of the EPAct, and the public comments

on the proposed rule. The Commission has considered and deliberated on the 12 factors identified in the EPAct, and the results of its consideration is set forth in Section II below. Additionally, the Commission specifically invited public comments on how these factors should be addressed in the rule. Many of the comments received both substantively and procedurally focused on the 12 factors. Those comments and the Commission's responses are also discussed in Section II.

It is important to note that the Commission was careful to set forth rule text in the final rule that does not compromise licensee security, but also acknowledges the necessity to keep the public informed of the types of attacks that nuclear power plants and Category I fuel cycle facilities are required to defend against. To this end, the final rule maintains a level of detail in the rule language that is generally comparable to the previous regulation, while updating the general DBT attributes in a manner consistent with the insights gained from the application of supplemental security requirements imposed by the April 29, 2003 DBT Orders, the EPAct, and consideration of public comments.

The final rule contains all of the requirements with which licensees must legally comply. More specific details (e.g., specific weapons, ammunition, etc.) are consolidated in adversary characteristics documents (ACDs) which contain classified or safeguards information. The technical bases for the ACDs are derived largely from intelligence information. They also contain classified or safeguards information that cannot be publicly disclosed. These documents must be withheld from public disclosure and made available only on a need-to-know basis to those who are otherwise cleared for access. Since the regulatory guides (RGs) and the ACDs are guidance documents that provide details to the licensees regarding implementation and compliance with the DBTs, these documents may be updated from time to time as a result of the NRC's periodic threat

reviews. The NRC has been conducting threat reviews since 1979. These threat reviews are performed in conjunction with the intelligence and law enforcement communities to identify changes in the threat environment which may, in turn, require adjustments of NRC security requirements. Future revisions to the ACDs would not require changes to the DBT regulations in 10 CFR 73.1, provided the changes remain within the scope of the rule text.

II. Analysis of Public Comments and Consideration of the 12 Factors of the EPAct

The proposed rule provided a 75-day public comment period which ended on January 23, 2006. The comment period was extended by another 30 days in response to a request from the Nuclear Energy Institute (NEI), an industry group, to allow additional time for review of the proposed rule because the comment period overlapped the year-end holidays. The extended comment period ended on February 22, 2006. A total of 919 comments were received. Sources for these include about nine hundred individuals, one county, thirteen citizen groups, one utility involved in nuclear activities, and two nuclear industry groups. The comments covered a range of issues, some of which were beyond the scope of this rulemaking in that they were specific to protective measures but did not relate to the adversary characteristics. The comments have been organized under three groups; Group I: Considerations of the 12 Factors in the EPAct, Group II: In Scope comments, which includes comments raising issues and concerns directly related to the contents of the DBT rule, and Group III: Out of Scope comments, which includes comments raising issues and questions that are not directly related to the DBT rule, although they are relevant to the security of nuclear facilities. Responses are provided in the following format:

Group I: Consideration of the 12 Factors in the Energy Policy Act

The Commission's considerations, public comments and responses to the public comments are provided for the 12 factors described in Section A.

Group II: In Scope Comments

Comments in Group II and III are organized under the following general categories. The Commission's responses to these comment categories are provided in Section B:

1. Definition of the Design Basis Threat
2. Applicability of the Enemy of the State Rule
3. Compliance with Administrative and Procedures Act (APA) Notice and Comment Requirements
4. Ambiguous Rule Text
5. Differentiation in Treatment of General and Specific License for ISFSI
6. Applicability of the DBTs to New Nuclear Power Plants
7. Consideration of the Uniqueness of Each Plant in application of the DBTs
8. Continued exemption of Research and Test Reactors from the DBT requirements
9. Changes in Security Requirements to be Addressed Under Backfit Rule
10. Compliance with the Paperwork Reduction Act
11. Adequacy of the Regulatory Analysis
12. Compliance with the National Environmental Protection Agency (NEPA)
13. Issuance of Annual Report Card on Individual Licensees

Group III: Out of Scope Comments

14. Federalization of Security
15. Force-on-Force Tests of Security

16. Screening of Workers in Nuclear Power Plants

17. Self-Sufficient Defense Capabilities

18. Security of Dry Cask Storage

19. Security of Spent Fuel Pools

20. Inherent Design Problems that make Reactors Vulnerable

A Comments Matrix has been provided in Appendix A, which references each topic with comments. The NRC's response to each topic is listed below:

Section A

Group I. Consideration of the 12 Factors in the Energy Policy Act

As discussed above, Section 170E of the AEA, as amended by Section 651(a) of the EPAct, directed the Commission to consider in the course of the DBT rulemaking, but not be limited to, the 12 factors specified in the statute. Many of the comments received by the Commission focused on one or more of these factors. Prior to discussing the substance of the 12 factors, the Commission notes that several commenters charged that the Commission violated Section 170E by not considering some of the 12 factors, and by deferring final consideration of some of the provisions to the final rule. Those commenters suggested that this not only violated the mandate of Section 170E, but also the Administrative Procedure Act (APA) by not providing adequate notice of the substance of the rule, and thus the rule should be withdrawn and re-proposed.

To be clear, Section 170E stated that the Commission "shall consider," but not be limited to, the 12 factors, when conducting the DBT rulemaking. The EPAct did not, however, require that the Commission explicitly include any of the 12 factors in the proposed or final rule text. The Commission did carefully consider, along with intelligence reports, vulnerability assessments, and other Commission-sponsored

studies, each of the 12 factors in formulating the final rule. Accordingly, a number of provisions or rule changes were adopted that specifically incorporate certain language used in the 12 factors. For instance, the final rule contains specific provisions related to multiple, coordinated teams of attackers (Factor 3), suicide attacks (Factor 5), insider assistance (Factors 4 and 8), and waterborne attacks (Factor 6). Additionally, based on the 12 factors, public comment, and other intelligence information, the Commission has decided to explicitly include a cyber threat as an element of the DBTs (Factor 2).

After careful consideration, the Commission also chose not to adopt elements related to some EPAct factors as part of the rule text. However, that decision should not be misconstrued as lack of consideration of the factors themselves. Nor should the Commission's statement in the proposed rule soliciting comments on "whether or how the 12 factors should be addressed in the DBT rule" be interpreted to mean that the Commission deferred consideration of the factors until after it received comments. Rather, the Commission proposed requirements that would require licensees to defend against threats the Commission considered appropriate at that time, subject to change in the final rule after further consideration of public comments.

Several commenters specifically charged that the Commission has deferred its consideration of air-based threats to the final rule, thus undermining stakeholders' abilities to know the Commission's position on that factor. On the contrary, the Commission has been evaluating the issue of air-based threats long before consideration of that factor was required by the EPAct. Also, the NRC's position on the necessity of imposing additional measures for protection against an airborne threat is

well documented.[1] Nevertheless, the Commission's evaluation of the airborne threat has been an ongoing process. At the time that the proposed rule was published, the Commission maintained its view that protection against airborne attack could best be provided by the strengthening of airport and airline security measures. Accordingly, the Commission did not propose to include a provision in the proposed rule that would require licensees to provide defense against an airborne attack. However, the lack of such a provision in the proposed rule text should not be construed that the Commission has deferred consideration of the issue until publication of the final rule. The Commission specifically sought comment on the issue in the proposed DBT rule and has remained open to changing its position. *See*, 70 FR 67382; November 7, 2005. In addition to being raised in PRM-73-12, the Commission has received numerous comments on the airborne threat. It has carefully considered those comments and has responded to them below.

Factor 1. The events of September 11, 2001

a. The Commission's Consideration: The events of September 11, 2001 have been central to the Commission's efforts in reevaluating the DBTs. As a result of these attacks, the DBTs were reevaluated immediately and additional requirements were imposed on licensees through the April 29, 2003 Orders. A number of revisions to the DBTs have resulted from consideration of the events of September 11, 2001. Those revisions include:

---

[1] On its public website, the Commission has set forth its position on a number of security issues, including aircraft attack. *See* "Frequently Asked Questions About NRC's Response to the 9/11/01 Events," at http://www.nrc.gov/what-we-do/safeguards/faq-911.html.

- Increased adversaries' willingness to kill or be killed,
- One or more adversary teams, and
- Multiple adversary entry points.

b. Public Comment: Several commenters specifically challenged the proposed rule's consideration of the events of September 11, 2001, expressing concern that the DBT rule does not require licensees to defend against a number of attackers comparable to the same number of terrorists (19) who participated in the attacks on September 11, 2001.

c. Response to Public Comment: The Commission disagrees with the comment. The Commission's consideration of the number of attackers comprising the DBT is discussed in more details below under Factor 3. However, with respect to the assertion that the number of attackers should be comparable to the number of September 11, 2001 attackers (19), the Commission notes that the official U.S. government terrorism report for 2001, "Patterns of Global Terrorism," states that the September 11, 2001 attacks consisted of "four separate but coordinated aircraft hijackings," not a single attack involving 19 assailants. In its annual terrorism report for 2001, the Federal Bureau of Investigation (FBI) considered the attacks as one act of international terrorism by "four coordinated teams of terrorists." Such seemingly antithetical information was just one part of a significant statistical analysis conducted by the NRC as part of the post-September 11, 2001 DBT process to determine the DBT adversary force size. In summary:

- NRC position: Disagrees with the comment.
- Action: No action required.

Factor 2. An assessment of physical, cyber, biochemical, and other terrorist threats

a. The Commission's Consideration: Although the DBT rule does not elaborate on the specifics of vehicle bomb size, numbers of adversaries, or exact types of weapons for operational security purposes, they are indeed robust. As explained above, the DBTs are the result of the NRC's continuous evaluation of current threats. That evaluation is not limited to a particular kind of threat, but naturally includes consideration of physical threats, cyber threats, and biochemical threats. The DBT rule therefore reflects the Commission's determination of the most likely composite set of adversary features against which private security forces should reasonably have to defend against.

To this end, the DBT rule has been amended in several significant respects to reflect the current physical, cyber, biochemical and other terrorist threats. For example, as discussed further below, the radiological sabotage DBT has been enhanced to reflect a capability to operate as one or more teams, attacking from one or more entry points. Additionally, in section 73.1(a)(1)(i)(c), the phrase "up to and including" was changed to simply "including" to provide flexibility in defining the range of weapons available to the composite adversary force.

One significant change to the rule related to physical threats includes the use of vehicles, either as modes of transportation or as vehicle bombs. Section 73.1(a)(1)(i)(E), for example, effectively expands the scope of vehicles available for the transportation of adversaries by deleting the reference to "four-wheel drive" and by adding water-based vehicles.

In addition, section 73.1(a)(1)(iii) (the land vehicle bomb provision) is similarly revised to delete the "four-wheel drive" limitation, and to add a capability that the vehicle bomb "may be coordinated with an external assault," maximizing its destructive potential.

Further, an entirely new capability has been added to the DBT involving a waterborne vehicle bomb, which also is encompassed in the coordinated attack concept.

With respect to biochemical threats, the Commission has also carefully considered those threats. The previous rule already contained provisions that provided the capability of using "incapacitating agents," and that capability has been retained in the final rule. There has been little threat information, however, that potential adversaries have acquired more lethal biological or chemical agents for use in facility assault scenarios, so the final rule does not reflect these kind of capabilities.

b. Public Comment: Although many of the public comments could generally be characterized as addressing Factor 2, only several comments specifically fell under this factor. One commenter stated that the NRC needs to engage independent experts to develop a comprehensive computer vulnerability and cyber attack threat assessment, which must evaluate the vulnerability of the full range of nuclear power plant computer systems and the potential consequences of these vulnerabilities. The commenter further suggested that the revised DBTs must incorporate these findings and include a protocol for quickly detecting such an attack and recovering key computer functions in the event of an attack.

Two other commenters stated that the regulations do not reflect protections against potential of explosive devices of considerable size, other modern weaponry, and cyber, biochemical and other terrorist threats. Another commenter did not believe the proposed DBTs protected against all conceivable attacks, such as launching a large explosive device from a boat, clogging the water intakes, dropping a conventional bomb into spent fuel pools, insider sabotage, etc.

c. Response to Public Comment: Regarding the cyber threat comment, the NRC

agrees with the statement submitted by the commenter and explicitly included a cyber threat as an element of the DBTs in the final rule. The basis for this addition, and implications of the rule change are discussed further in Section III. In addition, the proposed draft 10 CFR 73.55(m), "Digital Computer and Communication Networks," which soon will be released for public comment, contains proposed measures to mitigate the cyber threat.

With respect to the other comments regarding protection against explosives of considerable size and modern weaponry, as stated earlier, the details of the adversaries capabilities can not be specified in a public rule, but they are indeed substantial. Furthermore, the land vehicle bomb assault may be coordinated with an external assault, maximizing its destructive potential.

With reference to the final comment, the NRC does not intend the DBTs to represent "worst case" scenarios or all conceivable attacks. It is impossible to address all possible attack scenarios, especially those that would fall into a "worst case" category, because there is no theoretical limit to what attack scenarios can be conceived. Therefore, the NRC staff bases the DBT adversary tactics on those higher-probability tactics that have been observed in use, discussed, or trained for by potential adversaries. These tactics and all DBT provisions are submitted to an interagency review process where Federal law enforcement and intelligence community agencies comment and provide feedback. If changes develop in adversary tactics that could significantly impact nuclear facility security, the staff would request that the Commission consider these tactics for inclusion in the DBT provisions. In summary:

- NRC position: Agrees with one element of comment—cyber threat, disagrees with other two elements.

- Action: Final rule includes cyber attack as an explicit element of the DBTs. No other action required.

Factor 3. The potential for attack on facilities by multiple coordinated teams of a large number of individuals

a. The Commission's Consideration: The number of attackers, and the tactics used by those attackers, is now and has always been the core consideration of the DBT. Although the NRC obviously cannot comment on the size (specific number of attackers) of the DBT adversary force for operational security reasons, it can address the process by which these numbers are derived. As noted in the Commission's considerations for Factor 1, the size of the DBT adversary force and the number of assault teams were derived through a careful and deliberative process involving not only the NRC staff, but Federal law enforcement and intelligence community agencies using a variety of intelligence and unclassified sources. A statistical analysis was done on terrorist group size, looking at hundreds of terrorist attacks over several years, and it was compared with previous such group size analyses for changes in long-term trends. Large "outlier" terrorist events, while few in number, were included in this analysis. This statistical analysis was factored into a parallel analysis of known terrorist attacks against protected facilities (also few in number) and terrorist training, tactics and doctrinal manuals concerning armed assaults against facilities.

In addition, the NRC found that the vague qualifiers ("several persons" and "small group") in the previous adversary descriptions in 10 CFR 73.1 did little to add to the clarity of the rule, because the phrases are highly subjective. Thus the final rule now contains the more specific language "by an adversary force capable of operating as one

or more teams, attacking from one or more entry points." By revising the language in the rule, and eliminating the reference to "several persons" and "small groups," the NRC actually increased the potential flexibility of an adversary. The use of two or more adversary teams is not necessarily tactically advantageous to the attacking force in all possible scenarios. In some instances, the adversary force, as replicated in Force-on-Force (FOF) can, based on its analysis of the licensee's protective strategy, concentrate its force in a single team if necessary to best attack a facility. In other instances, a licensee's protective strategy may be most vulnerable to multiple teams of attackers attempting entry from different locations. In any event, the final DBT rule now provides enough flexibility to account for all of these scenarios.

b. Public Comment: Several commentators contend that for nuclear power plants, the regulations should provide protection against coordinated attacks by multiple large teams of up to two dozen sophisticated and knowledgeable adversaries.

c. Response to Public Comment: As stated above, the Commission has revised the rule to reflect these considerations and to provide maximum flexibility in developing threat scenarios. In summary:

- NRC position: Agrees partially with the comment.
- Action: No action required.

Factor 4. The potential for assistance in an attack from several persons employed at the facility

a. The Commission's Consideration: The Commission has always considered the threat of insider assistance to be a very real and dangerous threat. Thus, the DBTs have long contained a provision requiring licensees to protect against inside assistance. Also, other NRC regulations contain substantial requirements for access authorization

programs. (See, 10 CFR 73.56, Personnel Access Authorization Requirements for Nuclear Power Plants, and 10 CFR 73.57, Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees.) The final rule, however, has amended this requirement to expand the threat of insider assistance. For instance, 10 CFR 73.1(a)(1)(A) and 2(i)(A) add language indicating that the adversaries have "sufficient knowledge to identify specific equipment or locations necessary for a successful attack." This provision therefore suggests that such knowledge could be obtained from an insider who has such knowledge.

The inside assistance provision itself has also been revised. The final rule deletes the term "individual" to provide flexibility in defining the number of persons who may be involved in providing inside assistance.

b. Public Comment: One commenter stated that the insider attribute must include an active participant in an attack and should include the possibility of first responders and or National Guardsmen providing insider assistance.

c. Response to Public Comment: The staff agrees with part one of this comment. The capability of "active" insider assistance is clearly stated in both 10 CFR 73.1(a)(1)(i)(B) for radiological sabotage and 10 CFR 73.1(a)(2)(i)(B) for theft or diversion of strategic special nuclear material. Further, the "active" assistance capability has long been a component of the DBTs. The use of the conjunction "or" provides for increased tactical flexibility on the part of the adversary, based on the specific situation. It does not preclude an active insider in favor of a passive one.

NRC disagrees with the second part of this comment. National Guard, local law enforcement and other non-licensee security personnel already stationed at the owner-

controlled boundary or entry portals of some licensee facilities are not part of the licensee workforce and not subject to NRC regulatory authority, hence they are considered beyond the scope of the DBTs. Typically, these organizations have their own internal screening procedures to determine reliability, and NRC recognizes that those processes exist and provide some assurance against an insider threat to that organization. Furthermore, first responders, law enforcement and National Guard personnel are not given unescorted access to the Protected Area (PA).

First responders, law enforcement and other external security personnel responding to an emergency or security event at a site would do so according to pre-established emergency response protocols. If a particular responding organization had been penetrated by an adversary insider, then he/she would be considered an external adversary for purposes of the DBTs. As such, the adversary would be covered under this statement in the DBTs: "A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions," whereas the adversary would be considered to be conducting deception. In summary:

- NRC Position: Agrees with the first element of the comment, disagrees with the second element of the comment.
- Action: No action required.

Factor 5. The potential for suicide attacks

a. The Commission's Consideration: The final rule contains language reflecting the potential for suicide attacks. Language has been added to Section 73.1(1)(i)(A) and 73.1(2)(i)(A) indicating that potential adversaries have the attribute of a willingness to "kill or be killed."

b. Public Comment: No public comment received.

c. Response to Public Comment: No response required.

Factor 6. The potential for water-based and air-based threats

a. The Commission's Consideration: Certainly one of the most substantial considerations of the Commission, NRC licensees, the Federal government, and the public is the threat of airborne attacks against critical infrastructures. As stated below, the vast majority of comments received by the Commission on the proposed DBT rule regarded the airborne threat. The Commission has been evaluating the issue of air-based threats long before it was required by the EPAct, and its position on the necessity to add this capability to the DBTs prior to this rulemaking has been well documented. The Commission's evaluation of the airborne threat has been an ongoing process, and it has spent a significant amount of time and resources as part of this rulemaking in considering whether to make some type of airborne threat part of the DBTs. Ultimately, the Commission has determined that active protection against the airborne threat requires military weapons and ordinance that rightfully are the responsibilities of the Department of Defense (DOD), such as ground-based air defense missiles, and thus the airborne threat is one that is beyond what a private security force can reasonably be expected to defend against. This does not mean that the Commission is ignoring the airborne threat; merely that the responsibility for actively protecting against the threat lies with other branches of the Federal government, as it does for any U.S. commercial infrastructures.

Beyond active protection, the Commission believes that some considerations involving airborne attack relate to the development of specific protective strategies and physical

protection measures that are not within the scope of the DBTs. Deployment of protective measures such as no-fly zones, combat air patrols, and ground-based air defenses are undertaken by many other Federal agencies working on preventing and protecting critical infrastructure from terrorist attacks, including the U.S. Northern Command (USNORTHCOM) and North American Aerospace Defense Command (NORAD), the Transportation Security Administration (TSA), and the Federal Aviation Administration (FAA). The significant increase in aviation security since September 11, 2001 goes a long way toward protecting the United States, including nuclear facilities, from an aerial attack. Some of these improvements include:

- Criminal history checks on flight crew;
- Reinforced cockpit doors;
- Checking of passenger lists against “no-fly” lists;
- Increased control of cargo;
- Random inspections;
- Increased Federal Air Marshal presence;
- Improved screening of passengers and baggage;
- Federal Flight Deck Officer Program;
- Controls on foreign passenger carriers;
- Requirements on charter aircraft;
- Enhanced vigilance of flight training; and
- Improved coordination and communication between civilian and military authorities.

The deployment of ground-based air defense weapons would be a decision for the Secretary of Defense, not the NRC. However, the NRC believes that application of

ground-based air defense weapons would present significant command and control challenges, particularly relating to the time required to identify and confirm the presence of a hostile aircraft and to get permission to shoot it down. The potential for collateral damage to the surrounding community also would have to be considered. The FAA has issued a Notice to Airmen (NOTAM) strongly advising pilots to avoid the airspace above, or in proximity to, such sites as power plants (nuclear, hydro-electric, or coal), dams, refineries, industrial complexes, military facilities and other similar facilities. Pilots are warned not to loiter in the vicinity of these types of facilities.

In February 2002, the Commission, in addition to the actions of other Federal agencies, directed nuclear power plant licensees to develop specific plans and strategies to respond to a wide range of threats, including the impact of an aircraft attack. The NRC has continued to work with licensees on these issues and has inspected licensee actions to respond and implement mitigation strategies to limit the effects of such an event. The NRC has conducted detailed, site-specific engineering studies of a limited number of plants to gain insights on potential vulnerabilities of nuclear power plants to deliberate attacks involving large commercial aircraft. The results of these studies have confirmed the effectiveness of the February 2002 NRC-ordered mitigative measures, and have identified the need for some additional enhancements. For the facilities analyzed, the studies confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low. Even in the unlikely event of a radiological release due to a terrorist use of a large aircraft against a nuclear power plant, the studies indicate that there would be time to implement the required on-site mitigating actions. These results have also validated the off-site emergency planning basis. Nevertheless, on June 20, 2006, the NRC issued Orders to appropriate power reactor licensees requiring the implementation of key radiological

protection and mitigation strategies to reduce potential consequences from the loss of large areas of the plant due to large fires or explosions. (*See* in the Matter of Operating Power Reactor Licensees Identified in Attachment 1; Orders Modifying Licensees (Effective Immediately), 71 FR 36554; June 27, 2006.) Additional studies are being considered to further assess mitigative capabilities. The NRC will continue to coordinate with the Department of Homeland Security (DHS) on this initiative. (See Factor 9 for further discussion of a related topic, "The potential for fires, especially fires of long duration.")

Finally, in early March 2006, the NRC hosted an Interagency Aircraft Attack Tabletop Exercise at NRC Headquarters. Representatives from the DHS, the DOD/USNORTHCOM, and the FBI attended. The purpose of the exercise was to explore Federal responsibilities and interfaces, consistent with the National Infrastructure Protection Plan and National Response Plan, for terrorist incidents at nuclear power plants, with a focus on an aircraft attack on the facility. The tabletop exercise reconfirmed the respective responsibilities of the participating agencies (NRC, DHS, DOD, and FBI) for a nuclear plant aircraft attack and clarified protocols for response-related interagency communication and coordination.

Regarding a water-based attack, the final DBT rule contains two new provisions that account for such a capability, as discussed under Factor 2. These capabilities were included based on conclusions drawn from the NRC's continuing review of intelligence information and liaison with Federal law enforcement and intelligence agencies. Sections 73.1(a)(1)(i)(E) and 73.1(a)(2)(i)(E) add the capability to use water-based vehicles for transporting personnel and equipment to the proximity of vital areas, and Sections 73.1(a)(1)(iv) and 73.1(a)(2)(iv) add a new provision for a waterborne vehicle bomb assault. The NRC has concluded that defense against these new DBT provisions

will provide a high-assurance of protection against the waterborne threat.

b. Public Comment: Approximately 820 comments indicated that the "beamhenges" concept or similar barrier method of protection should be considered for protection against airborne attacks. Comments also indicated that a "no-fly" zone should be imposed around nuclear power plants and that ground based-air defense systems should be deployed to protect each site.

Further, multiple commenters expressed concerns regarding vulnerabilities of nuclear power plants and other licensed facilities to terrorist waterborne attacks. Commenters suggested that the revised DBTs should require nuclear power plants and other licensed facilities situated on navigable waterways to be equipped with visible, engineered physical barriers.

c. **Response to Public Comment**: As explained above, the Commission has spent considerable time and resources considering the threat of air and water attacks on nuclear facilities. Based on these considerations, the NRC has chosen a two-track approach to respond to their threat in order to assure adequate protection. First, the NRC has determined that active protection against the airborne threat rests with other agencies of the Federal government, such as NORTHCOM and NORAD, TSA, and FAA. These relationships have been tested through exercises, and NRC will continue to do so. Second, licensees have been directed to implement certain mitigative measures to limit the effects of an aircraft strike. To the extent that commenters have suggested the imposition of specific physical security measures such as the "beamhenges" concept, the NRC has considered and deliberated on the issue, but has rejected the concept. Furthermore, these measures are beyond the scope of the DBT rulemaking, because the DBT does not define protective strategies and security measures.

With respect to the water-borne attack threat, as discussed above, the DBT rule has been revised to reflect two new water-based capabilities. However, requirements of physical barriers for the protection of the nuclear power plants and other licensed facilities under waterborne attack are not in the scope of DBT rule. Requirements for physical barriers are addressed in a separate rulemaking to amend 10 CFR 73.55. The security requirements in the proposed rulemaking that would amend 10 CFR 73.55 address protective strategies and security measures for nuclear power plants and other licensed facilities under waterborne attacks, and require licensees to defend against the DBTs. (Proposed Rule, Power Reactor Security Requirements, 71 FR XXXX (3150-AG-63)). In Summary:

- NRC Position: Agrees with the water-borne comment. Disagrees with "no-fly" zones and "beamhenges" concept comments.
- Action: No action required.

Factor 7. The potential use of explosive devices of considerable size and other modern weaponry

a. The Commission's Consideration: As part of its consideration of Factor 2, the Commission assessed the potential use of explosive devices of considerable size and other modern weaponry. As such, the Commission notes that the DBTs have been revised to specifically reflect these two considerations. First, Sections 73.1(a)(1)(i)(C) and 73.1(a)(2)(i)(C) were amended to revise the phrase "up to and including" to simply "including" to increase the flexibility in defining the available range of weapons. Second, the vehicle bomb threat has been expanded to include waterborne vehicles. This Factor has been further articulated in Factor 2.

b. Public Comment: Refer to Factor 2.

c. Response to Comment: Refer to Factor 2.

In summary:

- NRC Position: Agrees with the comment.
- Action: No action required.

Factor 8. The potential for attacks by persons with a sophisticated knowledge of facility operations

a. The Commission's Consideration: As noted above under the discussion of Factor 4, Sections 73.1(a)(1)(i)(A) and 73.1(a)(2)(i)(A) added language indicating that the adversaries have "sufficient knowledge to identify specific equipment or locations necessary for a successful attack."

b. Public Comment: No public comment received.

c. Response to Comment: No response required.

Factor 9. The potential for fires, especially fires of long duration

a. The Commission's Consideration: The DBTs describe specific adversary characteristics against which licensees must be prepared to defend against. Fires, in contrast, are not adversary characteristics, but rather the result of a particular adversary action. Neverthless, the NRC considered fire to be a result of several possible events, both accidental and malicious in nature. The NRC conducted vulnerability assessments for some operating nuclear power plants in the 1970s and 1980s to establish the technical basis for security requirements. The NRC also routinely evaluated the potential impacts of terrorist attacks on power reactors as part of the FOF exercise

program on a plant-by-plant basis. After the terrorist attacks on September 11, 2001, the NRC promptly assessed the potential for and consequences of terrorists targeting a nuclear power plant, including its spent fuel storage facilities, for an aircraft attack, the physical effects of such a strike, and how compounding factors (e.g., fires, meteorology, etc.) would affect the impact of potential radioactive releases. As part of a comprehensive assessment, the NRC conducted detailed site-specific engineering studies of a limited number of nuclear power plants to assess potential vulnerabilities of deliberate attacks involving a large commercial aircraft. Additional Commission considerations are provided under the discussion of Factor 6, and a summary of the assessment study is available in a publicly available document.

b. Public Comment: One commenter stated that the proposed rule did not consider the potential for fires, especially fires of long duration, thereby, the proposed rule does not comply with the Congressional directive because it fails to mention the fire threat.

c. **Response to Public Comment:** The NRC disagrees with the statement submitted by the commenter. As stated above, the NRC considered fire to be a result of several possible threats. Adversary forces, bombs, and explosives can all result in fires, and potentials for fires have been considered during the DBT rulemaking process. The following is provided as background information related to this comment.

As part of a larger NRC effort to enhance the safety and security of the nations nuclear power plants, an initiative was undertaken as part of a February 2002 NRC order. The order, among other things, required licensees to look at what might happen if a nuclear power plant lost large areas due to explosions or fires. The licensees then were required to identify and later implement strategies that would maintain or restore cooling for the reactor core, containment building, and spent fuel pool. The requirements listed

in Section B.5.b of this order directed licensees to identify "mitigative strategies" (meaning the measures licensees could take to reduce the potential consequences of a large fire or explosion) that could be implemented with resources already existing or "readily available." The NRC held inspections in 2002 and 2003 to identify whether licensees had implemented the required mitigative strategies.

These inspections, as well as additional studies, showed significant differences in the strategies implemented by the plants. As a result, the NRC developed additional mitigative strategy guidance. The guidance was based on "lessons learned" from NRC engineering studies, and it included a list of "best practices" for mitigating losses of large areas of the plant. Each plant was requested to consider implementation of applicable additional strategies by August 31, 2005. The NRC inspected each plant in 2005 to review their implementation of any additional mitigative measures. The NRC is continuing to ensure licensees appropriately implement these measures.

Finally, aircraft attack, another threat likely to result in fires, was also considered, and studies analyzing the consequences successful commercial airline attacks were performed. In conducting these studies, the NRC drew on national experts from several DOE laboratories using state-of-the-art structural and fire analyses. The NRC also enhanced its ability to realistically predict accident progression and radiological release consequences. For the facilities analyzed, the studies found that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low. Even in the unlikely event of a radiological release due to terrorist use of a large aircraft, there would be time to implement mitigating actions and offsite emergency plans such that the NRC's emergency planning basis remains valid (*See* in the Matter of Operating Licensees Identified in Attachment 1; Order Modifying Licensees, 71 FR 36554; June 27, 2006.) Additional site-specific studies of operating nuclear power

plants are underway or being planned to determine the need, if any, for additional mitigating capability on a site-specific basis. In summary, the NRC considered the potential for fires during the DBT rulemaking process, as required by the EPAct.

- NRC position: Disagrees with the comment.
- Action: No action required.

Factor 10. The potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals

a. The Commission's Consideration: As stated in response to Factor 3, the Commission considered the potential for attacks on nuclear facilities by multiple coordinated teams of a large number of individuals. The number of attackers, and the tactics used by those attackers, is now, and has always been the core consideration of the DBTs. In addition, the Commission is considering the potential for attacks on spent fuel shipments by multiple coordinated teams of a large number of individuals. The Commission is planning to propose a rule on spent fuel shipments in the near future.

b. Public Comment: No public comment received.

c. Response to Public Comment: No response required.

Factor 11. The adequacy of planning to protect the public health and safety at and around nuclear facilities, as appropriate, in the event of a terrorist attack against a nuclear facility

a. The Commission's Consideration: The DBT rule does not include requirements imposing specific emergency planning considerations. Nevertheless, the Commission considered the implications of security-related incidents on emergency planning. As

part of those efforts, the NRC and DHS worked together to develop and improve federal initiatives, as well as security planning efforts. The NRC and DHS demonstrated effective coordination of integrated emergency preparedness programs through evaluations of licensee and State/local/tribal response capabilities at nuclear power plants and fuel fabrication facilities, and reviews of critical infrastructure preparedness and response plans for commercial nuclear power plants. Our combined efforts have resulted in specific enhancements to security-related emergency preparedness measures, and continued improvement in capabilities for licensees and offsite response organizations to respond to a wide spectrum of events.

b. Public Comment: No public comment received.

c. Response to Public Comment: No response required.

Factor 12. The potential for theft or diversion of nuclear material from such facilities

a. The Commission's Consideration: The DBT rule includes two separate components: the DBT of radiological sabotage, and the DBT of theft or diversion of formula quantities of special nuclear materials. Although the legal requirements of the radiological sabotage DBT and the theft or diversion DBT, found in 73.1(a)(1) and in 73.1(a)(2), respectively, are the same as stated in the rule, the ACDs and RGs are different in describing how power reactor and Category I fuel cycle facility licensees should implement and comply with the separate rules. These differences are classified and are not elaborated on here.

As stated in 10 CFR 73.55(a), power reactor licensees are only required to protect against the threat of radiological sabotage. Spent fuel is not an attractive theft or diversion target due to its large physical size and high thermal heat and radioactivity

(spent fuel is considered “self-protecting”.) As stated in Group III Comment No. 18 (Security of Dry Cask Storage) and 19 (Security of Spent Fuel Pools), NRC has required that licensees take additional security and mitigating measures against a radioactive release of spent fuel. However, NRC has authorized the Duke Energy Corporation, owner and operator of the Catawba plant, to burn four fuel assemblies of Mixed-Oxide (MOX) fuel at the Catawba plant on a test basis as part of its license amendment issued on March 3, 2005. MOX fuel technically meets the criteria of a formula quantity of Special Nuclear Material, in this case plutonium (Pu). As such, it would be subject to the DBT provisions of 73.1(a)(2) for theft or diversion. However, the NRC staff found that MOX fuel is not attractive to potential adversaries from a proliferation standpoint due to its low Pu concentration, composition, and form (size and weight). The MOX fuel consists of Pu oxide particles dispersed in a ceramic matrix of depleted uranium oxide with a Pu concentration of less than six weight percent. The MOX fuel assemblies are the same form as conventional fuel assemblies designed for a commercial light-water power reactor and are over 12 feet long and weigh approximately 1,500 pounds. A large quantity of MOX fuel and an elaborate extraction process would be required to yield enough material for use in an improvised nuclear device or weapon. On the “attractiveness” bases, the NRC staff found that the complete application of 10 CFR 73.45(d)(1)(iv), 73.46 (c)(1), 73.46(h)(3), 73.46(b)(3) - (b)(12), 73.46(d)(9), and 73.46(e)(3) for MOX fuel was not necessary and that the exemptions to these regulations are authorized by law, and will not endanger life or property or the common defense and security and that are otherwise in the public interest.

Furthermore, transportation of the MOX fuel assemblies to Catawba will be done by the Department of Energy’s (DOE’s) Office of Secure Transportation, which has legal responsibility for the MOX fuel assemblies until custody is transferred to the licensee.

Afterwards, the spent MOX fuel is cooled and stored like other spent fuel on site, and is subject to the radiological sabotage DBT while stored in the spent fuel pool inside the Protected Area of the plant.

b. Public Comment: No public comment received.

c. Response to Public Comment: No response required.

Section B

Group II. In Scope Comments

1. Defining the "Design Basis Threat"

a. Public Comment:

- Multiple commentators expressed concern that the NRC has not publicly defined or explained the "design basis threat." Specifically, commenters were unclear what the Commission means by the statement that the DBTs are based on a "determination as to the attacks against which a private security force can reasonably be expected to defend against." These commenters suggested that the Commissions's failure to articulate the DBT concept creates an ambiguity in establishing the division of responsibility between NRC licensees, and the DOD, or DHS. Several commenters suggested that if the NRC does not require plants to defend against air attack because it is unreasonable for a private security force to be able to do so, then it has no choice but to federalize security by requesting that DHS or the military assume full responsibility for the protection of nuclear power facilities.
- Other commenters suggested that the NRC's rationale for limiting the characteristics of the DBTs to the attacks against which a private security force could reasonably be expected to defend appears to be based on cost

considerations, which is not permitted for measures that are necessary for the protection of public safety.

- Other commenters representing the nuclear industry, while agreeing that the DBT scope must be clear, asserted that the DBT can not be greater than the largest threats against which private sector facilities can reasonably be requested to defend themselves, and threats beyond the DBT are reasonably the responsibility of the national defense system.

b. Response to Public Comment: The Commission has determined that the DBTs, as articulated in the rule, are based on adversary characteristics against which a private security force can reasonably be expected to defend. This formulation provides the Commission with the flexibility necessary to make reasoned, well-informed decisions regarding the DBTs. In contrast, detailed, prescriptive criteria would be unduly restrictive and detrimental to good governance.

With regard to the federalization of nuclear plants security forces, the Commission does not have the authority to federalize nuclear security forces and cannot demand deployment of military forces to protect nuclear facilities. Nor has Congress chosen to require such measures. As it has stated publicly many times, the Commission is confident that neither measure is necessary or even prudent. (*See, e.g.*, Testimony of Chairman Richard A. Meserve to the Committee on Environment and Public Works, United States Senate, dated June 5, 2002, available *at* *ht*tp://www.nrc.gov/reading-rm/doc-collections/congress-docs/congress-testimony/2002/ml021570116.pdf.) A primary reason for this is that the introduction of a federalized nuclear security force or military unit to provide day-to-day security would create serious command and control issues for plant management because it would essentially

establish two classes of employees at commercial nuclear facilities, both of whom would be responsible for reactor safety in the event of a terrorist attack. This could result in a serious reduction in the licensee's ability to ensure reactor safety. In contrast, the continued use of private nuclear security officers responsible to the licensee maintains a unitary command structure focused on a unitary objective. The tightly-regulated private nuclear security forces in use today are well trained on the unique security considerations specific to nuclear power facilities and through rigorous FOF training have proven themselves to be effective and reliable. These conclusions were documented when the Commission originally studied the issue in 1976 in a report to Congress titled the "Security Agency Study."

However, the Commission acknowledges that the use of private security forces to defend nuclear power facilities faces limitations. For instance, there are legal limitations on the types of weapons and tactics available to private security forces. Generally, nuclear security officers have access only to weapons that are available to civilians. Although authority recently granted the Commission under the EPAct of 2005 will allow the Commission to authorize the use of more sophisticated weaponry, the most powerful weapons and defensive systems will remain reserved for use only by the military and law enforcement. Thus, it would be unreasonable to establish a DBT that could only be defended against with weapons unavailable to private security forces. Nor could the Commission require licensees to defend against threats that it considers to be "Enemies of the State" as defined by 10 CFR § 50.13, and is discussed below.

These limitations on weapons and defensive systems available to private security forces do not, however, undermine the Commission's confidence in those forces to provide adequate protection. The defense of our nation's critical infrastructure is a shared responsibility between the NRC, the DOD, Federal and State law enforcement, and

other Federal agencies. A reasonable approach in determining the threat requires making certain assumptions about these shared responsibilities. Although licensees are not required to develop protective strategies to defend against beyond-DBT events, it should not be concluded that licensees can provide no defense against those threats. The Commission's regulations at 10 CFR 73.55(a) require that power reactor licensees' security programs provide "high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety." Within this requirement is the expectation that, if confronted by an adversary beyond its maximum legal capabilities, onsite security would not immediately be rendered ineffective but rather, would continue to respond with a graded reduction in effectiveness. The Commission is confident that a licensee's security force would respond to any threat, no matter the size or capabilities, that may present itself. The Commission expects that licensees and State and Federal authorities will use whatever resources are necessary for both DBTs and beyond-DBT events.

Several commenters felt that the DBT rule should define clearly demarcated boundaries where the responsibilities of the licensee end and those of the Government begin for defending nuclear facilities. In the Commission's view, establishing set boundaries demarcating a division of responsibilities is neither possible nor desirable. The better approach is for the Commission to continue its efforts to encourage licensees and Government agencies to integrate and complement their respective security and incident-response duties so that facilities subject to the DBTs have the benefit of all available incident-response resources during the widest possible range of security events. Currently, such integrated response planning efforts include prearranged plans with local law enforcement and emergency planning coordination. Licensees also must

comply with event reporting requirements to the NRC so that a Federal response is readily available, if necessary.

The DBT rule is also guided by the Commission's knowledge that, in addition to being among the most robust industrial facilities in the world, nuclear power plants are arguably the most physically secured industrial facilities. No other civilian industry security force is subject to as much regulatory oversight as that of the nuclear industry. Although it is impossible to fully understand the motives or planning processes of those who plan to commit malevolent acts, the Commission cannot ignore the fact that such high levels of security, relative to other critical infrastructure, most certainly serve as a deterrent to would-be attackers. History has demonstrated that terrorist groups generally seek out so-called "soft targets," not robust, heavily-secured facilities such as a nuclear power plant. In recent years, however, terrorists have shown an increasing proclivity and capability to attack more protected targets when necessary, demonstrating the attributes characterized in this DBT rule.

The Commission's own expertise in this field is also reflected in the DBTs. The Commission has over thirty years of experience regulating the physical protection of nuclear facilities. Throughout this period, the Commission has maintained constant vigilance, continuously evaluating and reassessing the threat faced by the nuclear industry and adjusting accordingly. Nevertheless, no nuclear facility in the United States has ever faced a serious attack by a malevolent actor or actors. The Commission cannot ignore this fact when evaluating the risk. Nor can the possibility of an attack be ignored because certain organizations or individuals have recently expressed interest in attacking nuclear facilities. The Commission's view is that the rule of reason should continue to govern assessment of the current threat. Singular incidents, no matter how tragic, destructive, or innovative, should not outweigh the informed judgment that comes

from decades of experience and a continued pragmatic approach.

To be clear, however, the DBTs are not defined by cost considerations, as suggested by several commenters. This argument appears based on the faulty premise that the Commission's core assumption of a "private security force" is determined through cost. Though true that the Commission may not consider economic factors in determining the level of adequate protection of public health and safety, the Commission has clearly set forth above that the bounds of the DBTs are set by the staff's threat assessments and coordination with other law enforcement and intelligence agencies, as well as the legal limitations on security forces available to licensees. These are the factors that are critical to the Commission's determination of the DBTs, not economic considerations faced by licensees. In summary:

- NRC position: Disagrees with the comments.
- Action: No action required.

2. Applicability of the Enemy of the State Rule

a. Public Comment:

- Several commenters also suggested that the proposed rule does not clearly distinguish between an "enemy of the state" as defined by 10 CFR 50.13, and the DBTs. They asserted that the phrase "enemy of the state" is ambiguous and can no longer be relied on to preclude the development of defensive measures at nuclear power plants. Those commenters again expressed concern that the division of responsibilities between the licensees and the national defense system are ambiguous.
- Other commenters argued that the Commission has failed to explain why the

DBTs exclude an “Al-queda-like terrorist organization” as an “enemy of the state” notwithstanding the Commission’s statements in the vehicle bomb rulemaking, which described the characteristics of an “enemy of the state,” and which seemingly would have included an Al-Qaeda like organization.

- Commenters representing industry stated that licensees are not and should not be required to defend against threats posed by enemies of the United States. They argued that the DBTs represent the largest threat against which a private security force can reasonably be expected to defend against, and that any escalation of this adversary would be inconsistent with 10 CFR 50.13. Such threats are properly the responsibility of the national defense establishment and other security agencies.

b. Response to Public Comment: The enemy of the state rule, 10 CFR 50.13, was promulgated in 1967 amid concerns that Cuba might launch missile attacks against nuclear power plants in Florida. That rule was primarily intended to make clear that privately-owned nuclear facilities were not responsible for defending against missile attacks or other attacks that typically could only be carried out by foreign military organizations. *See,* FR 32 13455; September 26, 1967. By contrast, the DBT rule does not focus on the identity, sponsorship, or nationality of the adversaries. Instead, it affirmatively defines a range of attacks and capabilities against which nuclear power plants and Category I fuel cycle facilities must be prepared to defend. An adversary force that falls outside of the range of attacks against which nuclear facilities are reasonably expected to defend are considered to be “beyond-DBT,” but not necessarily an “enemy of the state.” The Commission disagrees that any extension of the DBTs automatically conflicts with 10 CFR 50.13. The Commission may upgrade the DBTs in

response to changes in the threat environment without necessarily implicating 10 CFR 50.13. To be clear, "beyond-DBT" and "enemy of the state" are not equivalent concepts. In addition, improved response capabilities may become available to private security forces in the future. In that case, potential increases to the DBTs may be "reasonable to expect a private force to protect against" without coming into conflict with "enemy of the state." In summary:

- NRC position: Disagrees with the comments.
- Action: No action required.

3. Compliance with Administrative and Procedure Act (APA) Notice and Comment Requirements

a. Public Comment:

- Multiple commenters stated that sharing the ACDs with an exclusive group of parties constitutes a violation of the APA because the technical basis for the proposed rule is contained in those documents. Those commenters stated that the NRC should disclose the general and legal principles discussed in the exchange of the documents without releasing safeguards information. Another commenter expressed concern that the DBT rule is based on ex parte communications received from the nuclear industry after sharing the contents of the proposed rule only to certain parties, and that since the general public has no idea what general legal or technical principles were discussed in these private communications it could not intelligently comment on the proposed rule.
- Other commenters charged that the DBT rulemaking is simply codifying secret orders to avoid public scrutiny. Thus, they suggest that because the proposed

rule does not contain specifics of the DBTs, the NRC is free to change the specific requirements without notice to the public, effectively conducting a secret rulemaking in violation of the APA.

- Industry commenters suggested that because the ACDs and RGs contain all relevant requirements of the DBT rule, they should be incorporated by reference into the DBT rule to ensure adequate stakeholder participation in changes to the specific details of the DBTs. Otherwise, these commenters argue that the use of the ACDs and RGs has the potential for circumventing the APA and Paperwork Reduction Act.

b. Response to Public Comment: The Commission is confident that the rulemaking process for the DBT rule complies with the APA. As set forth in the statements of consideration to the proposed rule, the Commission has carefully balanced the public interest in awareness of the security considerations for the protection of special nuclear material and the need for meaningful comment with security interests related to the disclosure of specific details of DBT adversaries. *See*, 70 FR 67380, 67382, November 7, 2005. The result is a DBT rule that defines in reasonable detail a range of attacks against which licensees are required to defend. The DBT rule contains all of the requirements with which licensees must legally comply. No additional information is necessary to understand or to comment on the proposed DBT rule.

The ACDs and RGs are guidance documents containing Safeguards Information (SGI) and classified information, and describe how licensees can comply with the regulations. The ACDs and RGs are not regulations, and are not legally enforceable. The APA permits agencies to develop guidance documents like the ACDs and RGs without following notice-and-comment rulemaking requirements. *See,* 5 U.S.C. 551(b)(3)(A).

Changing the guidance in the ACDs or RGs based on changes to the threat environment would not change the requirements of the rule itself.

The text of the proposed rule provided ample information to enable meaningful comment on what the current level of protection for nuclear power plants and Category I fuel cycle facilities should entail. Members of the public can and have provided the Commission their views in this rulemaking on the number of attackers, amounts of explosives, and types of weapons that licensees should be required to defend against, even without having access to classified information or SGI. Therefore access to the ACDs and the RGs is not necessary to enable meaningful public comment on the proposed DBT rule.

One commenter suggested that it was improper for the Commission to share the draft ACDs and RGs with members of the nuclear industry but not members of the general public. The Commission shared the draft ACDs and RGs with licensees at the request of NEI before expiration of the initial comment period because NEI, in its capacity as the representative of the nuclear industry, had a specific need to know the information in order to assist licensees in planning and designing protective strategies capable of defending against the DBTs. We also shared with the States of New Jersey and Illinois that had established a need-to-know and obtained appropriate clearance. Other NRC stakeholders do not necessarily share this need to know, and therefore, have not been granted access to the classified and safeguards-information ACDs and RGs.

The Commission did not provide the draft ACDs and RGs to enable industry comments on the rule, nor has the Commission received or considered non-public comments on the rule. Unfortunately, language in a *Federal Register* document granting NEI's request for a 30-day extension of the comment period could be read to suggest otherwise. *See*, 71 FR 3791; January 24, 2006. To be clear, the NRC shared the draft ACDs and RGs with licensees because licensees (unlike other stakeholders) need that

guidance in order to develop their protective strategies, as is stated in the *Federal Register* document. It also shared these documents to get specific comments on the RGs and the ACDs that the NRC is producing in parallel with the rule. Licensees did not need the ACDs or RGs to comment on the rule itself, nor did anyone else. The Commission's decision to extend the public comment period at the same time that it provided classified and SGI guidance documents to licensees admittedly caused some confusion on this point. However, the Commission reiterates that no SGI or classified information is necessary to enable public comment, nor were any non-public comments received or considered over the course of this rulemaking. All of the comments received and considered in this rulemaking have been made publicly available.

Finally, the Commission disagrees that the ACDs and RGs should be incorporated by reference in the text of the final rule. As explained above, the ACDs and RGs are guidance documents. The legally-binding requirements are contained in the text of the rule. Incorporating these documents by reference would not only be inconsistent with that approach, but would potentially subject these documents to public disclosure based on the requirements of Section 552 of the APA, and the regulations of the Office of the Federal Register. In summary:

- NRC position : Disagrees with the comments.
- Action: No action required.

4. Ambiguous Rule Text

a. Public Comment:

- Several commenters stated that the continued use of the phrase "one or more teams" in the rule ignores the inherent ambiguity of this type of construction, as

identified in the Atomic Safety and Licensing Board's 2005 decision in the *Catawba* licensing proceedings. *See Duke Energy Corporation* ((Catawba Nuclear Station, Units 1 and 2), LBP-05-10, 61 NRC 241, 297 (2005).) The commenters argued that this construction, (i.e. use of the conjunction "or") permits licensees to select from one of two options (i.e. either one team or more teams), and thus permits licensees to develop their protective strategy ignoring the possibility of three teams or more. The commenters therefore suggested that the rule be revised to eliminate use of this ambiguous construction. One commenter suggested rule text that read "capable of operating in multiple teams, up to the maximum number of teams that can be formed from the adversary force, where a team has no fewer than two members."

b. Response to Public Comment: The Commission disagrees that the phrase "capable of operating as one or more teams" is ambiguous. Notably, the prior radiological sabotage DBT rule did not contain language requiring licensees to defend against multiple teams of adversaries, though the theft or diversion DBT did. The final rule adds a requirement to the radiological sabotage DBT that licensees protect against an adversary "capable of operating as one or more teams," and the theft or diversion DBT have been revised for consistency. By using the construction "one or more," the rule requires that licensees evaluate a wide range of possible attack scenarios when developing their protective strategies. Under the final rule, licensees must be able to defend against an attack from multiple entry points by a number of teams and/or individuals. Neither a protective strategy that is only capable of defending against a single team nor one that is only capable of defending against a number of smaller teams would meet the requirements of the rule. In summary:

- NRC position: Disagrees with the comments.
- Action: No action required.

5. Differentiation in Treatment of General and Specific Licenses for ISFSI

a. Public Comment:

- One commenter stated that the NRC did not provide a specific rationale in the proposed rule as to why a specific license ISFSI with security requirements arising from the security requirements in 10 CFR 72.182 should be subject to a different DBT than a general license ISFSI with security requirements arising from 10 CFR 72.212, effectively when nearly identical spent fuel in identical storage casks is stored at these two classes of licensees. The commenter requested that the NRC describe why these two types of ISFSIs should be treated differently from a DBT perspective in the final rule, or indicate that these licensees are subject to the same security requirements.

b. Response to Public Comment: The commenter is correct in noting that specifically-licensed and generally-licensed ISFSIs are treated differently in the current regulations, although they have equivalent security measures in place through orders. For example, the current regulation in 10 CFR 73.1(a) contains an exemption for specifically-licensed ISFSIs, subject to 10 CFR 72.182. However, the physical protection regulations for specifically-licensed ISFSIs, found at 10 CFR 72.180 and 72.182, do not require protection against the DBT, so it is unnecessary to exempt specifically-licensed ISFSIs from the DBT regulation. By contrast, generally-licensed ISFSIs are required to protect against the DBT for radiological sabotage by 10 CFR 72.212(b)(5), but by the same regulation, are granted exceptions to specific

requirements for protecting against the DBT. Ultimately, both generally-licensed and specifically-licensed ISFSIs have equivalent protective measures in place, including those imposed by the October 2002 order. The intent of this rulemaking was to update the DBTs applicable to power reactors and Category I fuel cycle facilities. Conforming changes were made to preserve the existing regulatory structure for other licensees. The NRC may consider future rulemakings to align the generally-licensed and specifically-licensed ISFSI requirements. In summary:

- NRC position: Agrees with the comments.
- Action: No action required.

6. Applicability of the DBT to New Nuclear Power Plants

a. Public Comments:

- Two commenters stated that the DBT for new nuclear power plants should be the same as for operating nuclear power plants. One commenter specifically stated that the proposed rule did not justify the adoption of different DBTs for new nuclear power plants. The commenter believes that the NRC has already set the DBTs at the level of the largest threat against which a private guard force can reasonably be expected to defend. Therefore, there is no reason to have a different set of DBTs for new nuclear power plants. The commenter expressed a concern that different DBTs for new plants could result in two different sets of DBTs for the same nuclear power plant site with a currently operating nuclear power plant.

b. Response to Public Comment: The NRC agrees with the commenters that the DBT should be uniformly applicable to new and currently operating nuclear power

plants. In fact, the NRC did not propose different DBTs for new nuclear power plants in the proposed rule. As stated by the Commission in the staff requirements memorandum on SECY-05-120, "Security Design Expectations for New Reactor Licensing Activities," the expectation is that new reactors will be designed and constructed to be inherently more secure with less reliance on other elements of a traditional security program. To assess the security of new reactors, the NRC is developing proposed requirements for new reactor licensees to submit security assessments as part of the their license application package. In summary:

- NRC position: Agrees with the comments
- Action: No action required

7. Consideration of the Uniqueness of Each plant in Application of the DBTs

a. Public Comment:

- One commenter stated that each nuclear facility is unique due to its location and surrounding population. Therefore, the DBT for each facility must have its own specific requirements. The DBT cannot be a one-size fits all program.

b. Response to Public Comment: The DBT rulemaking specifies threat characteristics, and does not specify or include requirements for any specific programs. Site-specific security requirements are embodied in site security plans and security measures. The NRC does not agree with the statement submitted by the commenter that the DBT for each facility must have its own specific requirements. Site-specific requirements are given consideration as to how each site protects against the DBT that are used by licensees to develop their physical security plans. The NRC considers the site-specific requirements when it reviews and approves the plans, and tests the

adequacy of the site-specific requirements when it conducts force-on-force exercises at nuclear power plants.

It should be noted that the DBTs are comprised of attributes selected from the overall threat environment. The technical bases for the DBTs are based on the NRC's periodic threat assessments performed in conjunction with the Federal intelligence and law enforcement communities for identification of changes in the threat environment. The assessments contain classified and safeguards information that cannot be publicly disclosed. The NRC believes that the DBTs should be uniformly applicable to all comparable nuclear facilities and will continue to ensure adequate protection of public health and safety and the common defense and security by requiring the secure use and management of radioactive materials. In summary:

- NRC position: Disagrees with the comments.
- Action: No action required.

8. Continued Exemption of Research and Test Reactors from the DBT Requirements

a. Public Comment:

- Two commenters stated that research reactors possessing Category I quantities of highly-enriched uranium (HEU) must provide protection against theft at the same level as any other Category I facility.

b. Response to Public Comment: The NRC disagrees with this comment. The NRC has made a policy decision that Research and Test Reactors (RTRs) who possess Category I quantities of Special Nuclear Material protect this material as specified in the physical protection requirements for non-power reactor fuel in 10 CFR 73.60(a)(e) and

73.67. Under 10 CFR 73.60, non-power reactor licensees who possess or use greater than five kg of HEU are exempt from the requirements in 10 CFR 73.60 (a)(e) if the HEU is not readily separable and has a total external radiation dose rate in excess of 100 rems per hour at a distance of three feet from any accessible surface without intervening shielding.

Furthermore, it should be noted that most RTRs possess limited quantities of radioactive material on-site, and that the nature and form of this material is not easily dispersed or handled. As a result, the NRC has determined that RTRs pose a relatively low risk to public health and safety from potential radiation exposure and has tailored the security requirements and oversight for these facilities consistent with their relatively low risk. The NRC requires that RTR licensees have security plans and procedures that employ a defense-in-depth philosophy, and reflect a graded approach which considers the attractiveness of the reactor fuel as a target, and the risk of radiological release. RTR security programs and systems provide for early detection and response to unauthorized activities. These programs also include control of access to facilities, security personnel patrol, monitoring of RTR facilities, and respones to indications of unauthorized penetrations or activities. RTRs also have emergency plans in place with the needed organizational structure, resources, and communications capabilities to respond to emergency situations.

Those RTRs that are still licensed to use HEU are either already scheduled to convert to low-enriched uranium (LEU) or have plans to do so. The DOE is the lead agency for converting RTRs to LEU fuel. The NRC has been working with the DOE to facilitate this effort. In summary:

- NRC Position: Disagrees with the comment.
- Action: No action required.

9. Changes In NRC Security Requirements to be Addressed Under the Backfit Rule

a. Public Comment:

- One commentator stated that the Backfit Rule requires that the NRC perform an analysis of changes in position. The commenter stated that the NRC has determined that a backfit analysis is not necessary in connection with the changes to the DBTs because the changes result from redefining the level of protection that should be regarded as adequate. The commenter further stated that such a determination should be supported by analysis, but the proposed rulemaking does not provide such an analysis, and each future change to the ACDs and RGs will require a separate backfit analysis.

b. Response to Public Comment: The Commission disagrees with the comment that the proposed rulemaking does not provide a documented evaluation of its decision. As stated in the *Federal Register* (*70* FR 67387), the NRC has determined, pursuant to the exception in 10 CFR 50.109(a)(4)(iii), that a backfit analysis is unnecessary for this rule. 10 CFR 50.109 states 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." 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 threatening 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 the security requirements previously imposed by the April 29, 2003 Orders, which applied only to existing licensees, should be made generically applicable. The Commission further finds that the rule redefines 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.

The Commission notes that it concurs with the commenter's position that documented evaluation should be performed when there are changes in ACDs and RGs necessitated by changes in the threat environment. In summary:

- NRC position: Disagrees with first element of the comment. Concurs with the second element of the comment.
- Action: No current action is required. Future changes in the ACDs and RGs will require a documented evaluation.

10. Compliance with the Paperwork Reduction Act

a. Public Comment:

- Several commentators stated that the Paperwork Reduction Act is circumvented by this approach. The proposed approach using RGs and ACDs to establish the details of the DBTs has the potential for circumventing the Paperwork Reduction Act, and avoiding proper regulatory analyses and backfit analyses. The rule provides broad requirements that lack details and provides the NRC with significant flexibility to change the details of the DBTs, which drives the design of protective measures and protective strategies without appropriate input from the

affected regulated licensees.

- The Paperwork Reduction Act Statement in the proposed rule states that: “This proposed rule does not contain new or amended information collection requirements subject to the Paperwork Reduction Act of 1995. See, 70 FR 67380; November 7, 2005. The commenter believes that this statement is incorrect and underestimates the impact on licensees due to future changes to the RGs and ACDs. The Paperwork Reduction Act Statement is flawed and should be revised.

b. Response to Public Comment: The DBT rule specifies threat characteristics used by licensees to design their protective strategies. The rule does not contain prescriptive measures to be adopted by individual licensees. The ACDs and RGs include the details of such threat characteristics. This approach has been adopted because the ACDs and RGs contain safeguards or classified information that cannot be disclosed in the public domain and would be useful to potential adversaries. This approach is not a circumvention of the Paperwork Reduction Act, but reflects the inherent dichotomy of the DBT rulemaking in trying to reach a balance between the needs for meaningful public participation and the requirement to protect safeguards and classified information, where public disclosure of specific attributes or details of security designs or protective measures would have the potential of making them ineffective.

The statement, “This proposed rule does not contain new or amended information collection.... Act of 1995," is accurate. The final rule consolidates the supplemental requirements put in place by the orders and the existing DBTs in 10 CFR 73.1(a), and does not impose additional burden for the licensees even though the rule contains a cyber threat as an additional attribute of the threat. This is because the licensees

subject to the DBTs were directed by the Interim Compensatory Measures (ICM) order (EA-02-026) to consider and address cyber safety and security vulnerabilities. In April 2003, the Orders (EA-03-086) and (EA-03-087) which supplemented the DBT contained language concerning the cyber threat. Licensees were subsequently provided with a cyber security self-assessment methodology, the results of pilot studies, and a guidance document issued by the NEI to facilitate development of site cyber security programs. The designated licensees have done so accordingly.

With respect to future changes to the rule or the ACDs, the Commission will comply with the requirements of the Paperwork Reduction Act. In summary:

- NRC position: Partially concurs with the comment.
- Action: No current action is required.

11. Adequacy of the Regulatory Analysis

a. Public Comment:

- A commenter stated that the Commission has prepared a draft regulatory analysis on this proposed regulation. The analysis examines the costs and benefits of the alternatives considered by the Commission. The Commission requested public comment on the draft regulatory analysis. The regulatory analysis is based on an incorrect premise and should be revised. A statement in the Regulatory Analysis states that “Impacts upon the licensees from this proposed rule would be minimal. Because the adversary characteristics would remain consistent with those promulgated by orders, no technical changes will be required. Licensees may need to update references in their security plan documentation, which could be accomplished without NRC review and in

conjunction with future plan updates." One commenter believes that this statement is incorrect and underestimates the impact on licensees.

b. Response to Public Comment: The Commission disagrees with the commenter that the regulatory analysis is based on an incorrect premise and should be revised. The regulatory analysis contained in the proposed rule stated that "The proposed regulatory action would not involve imposition of any new requirements, and would not expand the DBTs beyond the requirements in place under NRC regulations and orders." Consequently, the proposed DBT amendments would not require existing licensees to make additional changes to their current NRC-approved security plans. This premise was correct then and is correct even now as a cyber threat is explicitly included as an attribute of the final rule. Even though the regulatory action involves the imposition of a cyber threat as an explicit requirement, this does not impose additional burden for the licensees. This is because, as stated above in response to Factor No. 10, the licensees subject to the DBTs were directed by the ICM order (EA-02-026) to consider and address cyber safety and security vulnerabilities. Licensees were subsequently provided with a cyber security self-assessment methodology, the results of pilot studies, and a guidance document issued by the NEI to facilitate development of site cyber security programs, and the designated licensees have done so accordingly. This additional requirement in the final rule does not expand the DBTs beyond the requirements currently in place under existing NRC regulations and orders. Consequently, DBT amendments will not require existing licensees to make additional changes to their current NRC-approved security plans. However, the NRC acknowledges that any future changes to the DBTs may affect the ACDs and RGs, and could possibly affect the licensees' security plans that would require either NRC's

approval or official communications noting the changes to the NRC. This may also impose additional burden to the licensees. In such events, the regulatory analysis would be changed accordingly. In summary:

- NRC Position: Disagrees with the comment.
- Action: Regulatory Analysis to be changed when there is change in the threat environment in the future.

12. Compliance with the National Environmental Protection Act (NEPA)

a. Public Comment:

- Several commenters stated that the proposed rule fails to satisfy NEPA, and the NRC must prepare an Environmental Impact Statement (EIS) for the proposed rule because this is a major federal action significantly affecting the quality of the human environment. These commenters stated that the action is significant because "the NRC's limitations on the scope of adversaries against which 'a private security force could reasonably be expected to defend' bears directly on the degree to which public health and the environment will be protected against the impacts of accidents caused by terrorist attacks." Further, commenters suggested that the NEPA commenting process would be a better forum to disclose and discuss the policy considerations associated with development of the DBTs.

b. Response to Public Comment: The Commission disagrees that this rulemaking requires the completion of an EIS, and that the NEPA commenting process would provide a better forum for discussion of sensitive security issues. The NEPA and the Commission's regulations at 10 CFR 51.20(a)(1) only require preparation of an EIS if

the proposed action is a major Federal action significantly affecting the quality of the human environment. The Commission prepared an environmental assessment (EA) for the proposed rule and found that there would be no significant environmental impact associated with implementation of the proposed rule if adopted; and therefore, concluded that no EIS was necessary. See 70 FR 67387; November 7, 2005. NEPA only requires that the Commission consider the "reasonably foreseeable" environmental effects of its actions in determining whether an EIS is necessary. *See*, 40 CFR.1508.8(b). Effects that are remote, speculative, or embody the worst-case outcome of a particular action do not require an EIS. The Commission has determined that the potential environmental effects of terrorist attack on a nuclear facility are remote and speculative. [*See*, In the Matter of Private Fuel Storage, L.L.C. (Independent Spent Fuel Storage Installation), CLI-02-25, 56 NRC 340, 348-349 (2002).][2] Thus, the staff has not been required to evaluate the highly-speculative impacts on the environment of a postulated terrorist attack at a nuclear facility. The consequences of a terrorist attack cannot be said to be "an effect" of this rule, and hence analyzing the effects of a terrorist attack would be incredibly speculative, if not impossible. The staff would first be required to engage in guesswork as to the likelihood of an attack. Even if it could theoretically do this, the staff would also have to postulate limitless combinations of DBT adversaries to determine which combinations, if successful, would have a significant

---

[2]The Commission recognizes that its position on the necessity of a terrorism analysis as part of an environmental review has been called into question by a recent decision in the 9th Circuit Court of Appeals. *See San Luis Obispo Mothers for Peace v. NRC*, 449 F.3d 1016
(9th Cir. 2006). However, a determination that the potential environmental effects of a terrorist attack as a result of the licensing of an intermediate Spent Fuel Storage Installation should be considered, does not necessarily lead to the conclusion that such considerations should also be considered as part of agency rulemaking action.

impact on the environment. NEPA does not require such endless inquiry.

The Commission does not agree that the NEPA process would provide a better forum for disclosure and discussion of the DBT rule than this rulemaking action. It is not exactly clear how publishing an EIS for public comment would result in the disclosure of additional information because NEPA does not provide any other mechanism by which additional information on a proposed rule could be obtained by commenters. Nor does the mere desire by a member of the public to have access to additional information on a particular agency action mandate that the agency conduct a full EIS. All information necessary for public comment on the proposed rule has been made available and therefore no greater level of detail contained in the ACDs and RGs would be discussed in the NEPA comment process. The Commission's public comment process in developing an EIS is not a forum for sensitive security issues. The Commission has determined that "the public interest would not be served by inquiries at NRC hearings and public meetings into where and how nuclear facilities are vulnerable, how they are protected and secured, and what consequences would ensue if security measures failed at a particular facility." [*See,* In the Matter of Private Fuel Storage, L.L.C. (Independent Spent Fuel Storage Installation), CLI-02-25, 56 NRC 340, 354-355 (2002).] In summary:

- NRC Position: Disagrees with the comment.
- Action: No action required.

13. Issuance of Annual Report Card on Individual Licensees

a. Public Comment:

- One commenter stated that the NRC should publish an annual report card assessing specific plant performance to defeat attacks in ongoing "table top" and

mock “force-on-force” exercises.

b. Response to Public Comment: The NRC partially agrees with the statements submitted by the commenter. The detailed results of security-related drills and exercises are, and will remain, protected as safeguards information because this information can provide insights to potential adversaries in planning of attacks. However, Section 651 of the EPAct required that the Commission submit two annual reports to the Congress, one classified and another unclassified, describing the results of the Commission’s force-on-force exercises and related corrective actions. The Commission recently submitted the first set of such reports to Congress. It should be noted that the public can obtain unclassified information from annual reports to the Congress. Through these reports, the NRC provides information regarding the overall security performance of the commercial nuclear power plants to keep Congress and the public informed of the NRC's efforts to help protect our Nation's electric power infrastructure against terrorist attacks. In addition, the NRC recently revised its policy on public availability of security inspection results. Therefore the existence of inspection findings for a specific site’s FOF exercises will be identified in the publicly available cover letter transmitting the inspection results to the licensee. In summary:

- NRC Position: Partially agrees with the comment.
- Action: No action required.

Group III. Out of Scope Comments

Though the following topics and comments are pertinent to the security issues of nuclear facilities, they are not directly related to the DBT rulemaking. The DBT rule specifies general threat characteristics, but does not specify protective strategies and

security measures to defend against and thwart attacks, accordingly the following questions are deemed outside the scope of this rulemaking. However, relevant information is provided as background material to facilitate a better understanding of the existing mechanisms in place, and answer the underlying questions and issues raised in the following public comments.

14. Federalization of Security

a. Public Comment: Commenters stated that the proposed rule should indicate that the threat of an air attack exceeds the defensive capabilities of a plant's security forces, and the Federal government should either take over the security of the plant; and/or integrate the response from local, State, and Federal government resources.

b. Response to Public Comment: The Commission disagrees with the comment. Federalization of nuclear power plant security is outside of the scope of the proposed rule. However, the following background information is provided for a clearer understanding of the issues involved, and the rationale of the Commission's position. The issue of a Federal protective security force to provide protection at commercial power reactors was initially studied by the NRC and documented in a report to Congress called the Security Agency Study, completed in August 1976. The study found that the "...creation of a Federal guard force would not result in a higher degree of guard force effectiveness than can be achieved by the use of private guards, properly trained, qualified, trained and certified by the NRC." Shortly after September 11, 2001, this issue was again raised. The NRC continues to support the concept that a private security guard force with special emphasis on performance based training and full accountability is the best approach to securing our Nation's commercial nuclear

facilities. The security for nuclear facilities should be addressed in the context of the protection of other sensitive infrastructure. Society should allocate its security resources according to the relative risks, and, as a result, the separation of nuclear facilities from all other types of sensitive infrastructure will fragment the analysis inappropriately.

Past legislation proposed that the NRC establish a security force for sensitive nuclear facilities. Current security forces at sensitive nuclear facilities are well-trained, well paid, and have high retention rates. This is in sharp contrast to airport security before the recent improvements. There have been no failures in nuclear plant security of the type that has plagued the commercial airline industry and thus, no need for such radical change. This change would bring about a fundamental shift in the responsibility and mission of the NRC, diverting the agency from being an independent regulator of nuclear safety and security to being a provider of nuclear security. This could create command and control issues because it would establish two classes of employees at nuclear sites; licensee staff to ensure the safe operation of the reactors and federal staff to ensure security. This could lead to conflicts and confusion in emergency situations, which would diminish nuclear safety.

The change would serve to increase the Federal Budget needlessly. Presumably, given the enhancement in the security threat which the guard force would be required to defend against, the NRC would be required to hire more guards than currently exists at sensitive nuclear facilities (more than 7,000 new federal workers, which is more than twice the number of staff now employed by the NRC.) These new workers would have to undergo extensive background checks, be trained and qualified, and be armed and equipped. The training of this force alone would likely overload any Federal law enforcement agency's training capability. Moreover, presumably the NRC would have to assume the responsibility for establishment of new security barriers and

communications capabilities at the nuclear facilities (which by itself raises complicated issues associated with the interplay of security barriers and safety considerations.) The NRC estimates that the additional cost to the Federal government to implement these changes may well be over $1 billion a year.

Supplementing the guard force with Federal forces inside the plant areas raises similar concerns. National Guard forces and local/state law enforcement units have been used successfully at a number of facilities to provide additional security external to the plants when deemed necessary, circumventing difficult command and control issues. Such an external capability can more easily be "surged" in time of crisis. In sum, the Commission does not believe such a change is needed. In the Commission's view, the qualified, trained, and tightly regulated private guard forces at nuclear plants should not be replaced by a new Federal security force. In summary:

- NRC position: Disagrees with the comment.
- Action: No action required.

15. Force-on-Force (FOF) Testing of Security

a. Public Comment: Several commenters stated that security and FOF exercises must be upgraded in order to demonstrate a high degree of confidence that site security forces are able to repel an assault like the September 11, 2001, attack. In addition, under Section 651(a)(1)(b) of the EPAct, the NRC shall mitigate any potential conflict of interest that could influence the results of a FOF exercise. In some instances, the same contractor had supplied both the security guards as well as the mock terrorists.

b. Response to Public Comment: The requirements related to FOF testing are outside the scope of this rule. However, the following is provided as background

information pertinent to this comment.

The NRC FOF exercise program is designed to provide a realistic evaluation of the proficiency of licensee security forces against a threat consistent with the supplemented DBTs issued by the Commission's April 29, 2003 order. Following the attacks of September 11, 2001, the agency has expanded and refined its FOF program to make the exercises more realistic. These changes have significantly increased the level of complexity for each exercise in terms of planning, preparation, and logistical support. The NRC agrees that a credible, well-trained, and consistent mock adversary force is vital to the NRC's FOF program. Therefore, the NRC has worked with the nuclear industry to develop a composite adversary force (CAF) that is trained to the standards issued by the Commission. The new CAF has been used for all FOF exercises conducted after October 2004 and represents a significant improvement in ability, consistency, and effectiveness over the previous adversary forces. The NRC continues to evaluate the CAF at each exercise using rigorous NRC performance standards.

The CAF is currently managed by a company (Wackenhut) that provides much of the security for U.S. nuclear power plants and is, therefore, well-versed in the security operations of nuclear power plants. The NRC recognizes that there may be a perception of a conflict of interest where the management company cannot adequately test either the CAF or the plant security force. The NRC established a clear separation of functions between the CAF and plant security force to ensure an independent, reliable, and credible mock adversary force. In addition, the CAF composition includes security officers that are not employed by Wackenhut and no member of the CAF may participate in an exercise at his or her home site.

It is important to emphasize that the NRC, not the CAF, designs, runs, and evaluates the results of the FOF exercises. Because the CAF does not establish the exercise

objectives, boundaries, or timelines, and the CAF's performance is subject to continual observation and evaluation by the NRC and its contractors, the agency controls the exercise. If the industry is unable to maintain an adequate and objective CAF that meets the standards mandated by the NRC, the NRC will take the necessary actions to ensure the effectiveness of the force-on-force evaluation program. The NRC is developing requirements for the performance of FOF testing as well as implementing EPAct requirements for the mitigation of conflict of interest in a separate rulemaking. In summary:

- NRC Position: Disagrees with the comment.
- Action: No action required.

16. Screening of Workers in Nuclear Power Plants

a. Public Comment: One commenter stated that the NRC must be able to regulate or at least oversee the initial and follow-up screening of temporary and permanent workers who will have access to the reactor vessel, the spent fuel pool, and the related valves, generators, pumps, electrical systems, and miles of piping that are required for the plant's operation and are vulnerable as terrorist targets.

b. Response to Public Comment: The DBT rule does not regulate or oversee specific programs. Instead, it defines the general threat that licensees must be able to defend against with high assurance. Accordingly, NRC regulation or oversight of screening of workers at nuclear power plants is outside the scope of this rule.

However, it should noted that the NRC requires licensees to have an access authorization program that meets NRC requirements. 10 CFR Part 73.56, "Personnel access authorization requirements for nuclear power plants," requires all 10 CFR 50 and 52 licensees to include the required access authorization program as part of their site

Physical Security Plan. Specifically, 10 CFR 73.56 states that the licensee is responsible for granting, denying, or revoking unescorted access authorization to any contractor, vendor, or other affected organization employee. The requirements in that program are intended to ensure that personnel granted unescorted access to vital areas of a nuclear power plant are trustworthy and reliable, and do not constitute an unreasonable risk to the health and safety of the public, including a potential to commit radiological sabotage. In summary:

- NRC Position: Agrees with the comment.
- Action: No action required.

17. Self-Sufficient Defense Capabilities

a. Public Comment: Two commenters stated that in some regions, notably in large metropolitan areas, communication and transportation modes make it impossible to provide outside help in time to aid in facility defense following a terrorist attack.

b. Response to Public Comment: The capabilities of offsite responders are beyond the scope of this rule. However, the following provides an overview of the existing programs and policies in place for addressing issues raised in this comment.

After the September 11, 2001 attacks, the NRC has worked with licensees, the DHS, and State and local governments to improve the capabilities of first responders as part of the National Infrastructure Protection Plan. Part of this program includes conducting Comprehensive Reviews of commercial nuclear site security. The Comprehensive Review is a government and private sector analysis of critical infrastructure facilities to determine the facilities' exposure to potential terrorist attack, the consequences of such an attack, and the integrated prevention and response capabilities of the owner/operator, local law enforcement, and emergency response organizations.

The results are used to enhance the security posture of the facilities and community first responders by using short-term improvements in equipment, training, and processes; and informing longer-term risk-based investments and science and technology decisions. In less than a year, comprehensive reviews have already resulted in numerous benefits to identify readily adaptable, low-cost protective measures for increased readiness and preparedness in the event of a terrorist attack or natural disaster. The nuclear sector was the first of the sectors to participate in these reviews. Because commercial nuclear reactors are generally perceived to be high consequence assets, a number of Federal agencies were directed to complete various assessments involving these facilities. Although recognizing that nuclear plants are the best-protected assets of our critical infrastructure, those Federal agencies and the nuclear industry also recognized the value of a unified, collaborative effort to enhance the protection of these vital assets. In summary:

- NRC Position: Disagrees with the comment.
- Action: No action required.

18. Security of Dry Cask Storage

a. Public Comment: Multiple commenters expressed concerns regarding vulnerabilities of dry cask storage at nuclear power plants under terrorist attacks. The commenters suggested that dry cask storage should be protected by:

(i) Separation with a minimum spacing of 50 yards between each cask,

(ii) Hardening with beamhenge, and/or

(iii) Burial in earthen mounds.

One commenter stated that the NRC must require berming of dry storage casks as part of the DBT.

b. Response to Public Comment: The Commission disagrees with the commenters' statements. However, design basis and vulnerabilities assessment of dry cask storage facilities are provided below as background information for better understanding of existing requirements.

Dry cask storage facilities (e.g., independent spent fuel storage installations (ISFSIs)) at nuclear power plants are designed to protect against external events such as tornados, hurricanes, fires, floods, and earthquakes. The standards in 10 CFR Part 72 Subpart E, "Siting Evaluation Factors," and Subpart F "General Design Criteria," ensure that the dry cask storage designs are very rugged and robust. The casks must maintain structural, thermal, shielding, criticality, and confinement integrity during a variety of postulated external events including cask drops, tip-over, and wind driven missile impacts.

After the terrorist attacks of September 11, 2001, the Commission initiated a program in 2002 to assess the capability of nuclear facilities to withstand terrorist attacks. As part of the program, the Commission analyzed the performance of ISFSIs under aircraft attacks and has evaluated the results of detailed security assessments involving large commercial aircraft attacks, which were performed on four representative spent fuel casks. The large aircraft impact studies included structural analyses of the aircraft impact into a single cask and the resulting cask-to-cask interactions. Those evaluations indicate that it is highly unlikely that a significant release of radioactivity would occur from an aircraft impact on a dry spent fuel storage cask.

The Commission is finalizing the security assessments for a number of representative spent fuel storage casks for additional types of attacks and weaponry (including ground attacks), and will continue to evaluate the results of the ongoing assessments. Based upon these results and any other new information, the Commission will evaluate whether any change to its spent fuel storage policy is warranted. The Commission

issued a security order for ISFSIs in October 2002, and required the licensees to consider implementing additional enhancement measures for dry cask storage. These enhancements to security included increased vehicle standoff distances, additional security posts, and improved coordination with law enforcement and intelligence communities, as well as strengthened safety-related mitigation procedures and strategies. In summary:

- NRC Position: Disagrees with the comment.
- Action: No action required.

19. Security of Spent Fuel Pools

a. Public Comment: Four commenters expressed concerns regarding vulnerabilities of spent fuel storage pools at nuclear power reactors under terrorist attacks. The comments referenced the summary of the study performed by the National Academy of Science (NAS) which indicated that a terrorist attack on spent fuel pools is a credible threat and may lead to a release of a large amount of radioactive materials to the environment if it were successful. One comment specifically stated that not only is the NRC's response to the findings of the NAS study slow, but also, that the NRC has no intention of addressing these risk issues. It further stated that the apparent absence of a concerted spent fuel security program in the revised DBT is further evidence of the NRC's failure to recognize and address the problem.

b. Response to Public Comment: Security program requirements are subject of another rulemaking, namely 10 CFR 73.55. Accordingly, the need for a concerted spent fuel security program in the revised DBT is beyond the scope of this rule. In addition, the Commission disagrees with the statements submitted by the commenters. The following is provided as background information pertinent to these comments.

The NRC has taken numerous actions to enhance the security of spent nuclear fuel, and will take appropriate additional action as necessary as a result of on-going evaluations. Before September 11, 2001, spent fuel was well protected by physical barriers, armed guards, intrusion detection systems, area surveillance systems, access controls, and access authorization requirements for employees working inside the plants. After September 11, 2001, the NRC has significantly enhanced its requirements and licensees have significantly increased their resources to improve security at spent fuel facilities at nuclear power plants. For example, the NRC's February 25, 2002 Order to power reactor licensees dealt with spent fuel pool cooling capabilities in the event of a terrorist attack.

The NRC also initiated a program in 2002 to assess the capability of nuclear facilities to withstand a terrorist attack. The early focus of that program was on power reactors, including spent fuel pools. As the results of that program became available, in February 2005 the NRC provided power reactor licensees additional guidance on the implementation of the February 2002 Order regarding spent fuel mitigation measures. The power reactor licensees responded to these additional specific recommendations in May 2005.

The NRC is working with industry to conduct additional plant-specific damage assessments for a range of potential attack scenarios. The NRC continues to evaluate spent fuel pool security in FOF exercises, which the NRC conducts at least once every three years at each power reactor site. The results of security assessments completed to date clearly show that storage of spent fuel in both spent fuel pools and in dry storage casks provides reasonable assurance that public health and safety, the environment, and the common defense and security will be adequately protected. In summary:

- NRC Position: Disagrees with the comment.

- Action: No action required.

20. Inherent Design Problems that make Reactors Vulnerable

a. Public Comment: One commenter stated that the present DBTs ignore vulnerabilities inherent in the design of nuclear facilities. The commenter stated that the NRC has granted exemptions from certain safety regulations (e.g., Appendix R fire protection standards) to many licensees that present obvious and unacceptable vulnerabilities. The commenter stated that the vulnerability of fire-safety related pump rooms at a nuclear power plant under an attack scenario was disregarded, although the probability of an accident resulting from an accidental fire was reduced. The commenter further related the documentation of concerns of vulnerabilities regarding inherent design problems through numerous petitions and allegations to the NRC.

b. Response to Public Comment: The Commission disagrees with the commenter's statement. The Commission is confident that the designs of currently operating reactors are safe, and provide adequate security protection. Moreover, it should be noted that inherent design vulnerabilities of nuclear facilities are beyond the scope of this rule, since the DBTs specify adversary characteristics and do not specify specific protective measures, such as design features. However, the commenter should be informed that the NRC is undertaking several separate rulemakings as an effort to mitigate this concern. For instance, the Commission has proposed a rule that would amend its regulation related to security requirements for power reactors, [Proposed Rule, Power Reactor Security Requirements, 71 FR XXX (3150-AG-63).] In addition, the Commission is also proposing to add new requirements to its regulations requiring applicants to assess specific design features that would be incorporated into the final design to support overall security effectiveness of nuclear power plants, [Proposed Rule,

New Power Reactors/Security Assessment, 71 FR XXX (XXX-XX-XX).]

With respect to the statement concerning the petitions and allegations documented and submitted to the NRC, the NRC will provide proper responses to them as received. In summary:

- NRC Position: Disagrees with the comment.
- Action: No action required.

III. Summary of Specific Changes Made to the Proposed Rule as a Result of Public Comment

One change is being made to the proposed rule which adds a cyber threat as an explicit element of the DBT rule for both external and internal adversaries.

The DBT requirements in 10 CFR 73.1 did not specifically include the threat of a cyber attack. However, the cyber threat was implied in the draft 10 CFR 73.1 issued for public comment in the Federal Register on November 7, 2005, most notably in sections 10 CFR 73.1(a)(1)(i)(B), (1)(ii), (2)(i)(B), and (2)(ii). Under Section 651(a)(2) of the EPAct of 2005, Congress directed NRC to consider making an "assessment of physical, cyber, biochemical, and other terrorist threats" when writing the revised rule. In addition, one commenter specifically referred to the need for the DBT rule to contain requirements pertaining to cyber attack capabilities.

The NRC has some history of requiring licensees to evaluate cyber vulnerabilities. In February 2002, licensees subject to the DBTs were directed by the ICM Order (EA-02-026) to consider and address cyber safety and security vulnerabilities. In April 2003, the Orders (EA-03-086 and EA -03-087) which supplemented the DBTs contained language concerning the cyber threat. Licensees were subsequently provided with a cyber security self-assessment methodology and the results of pilot studies, as well as

additional guidance issued by the nuclear industry, in order to facilitate development of site cyber security programs.

NRC staff liaison with the U.S. Intelligence and Law Enforcement Communities indicates that the cyber threat is an enduring one, and likely will increase both in capability and frequency in the future. In light of this threat, the cyber security programs already initiated by the industry, the proposed draft 10 CFR 73.55(m), "Digital Computer and Communication Networks," which soon will be released for public comment, and the requirements of the EPAct of 2005, the Commission decided to use the current 10 CFR 73.1 rulemaking process to ensure consistent application of formal cyber threat language in the regulations.

IV. Section by Section Analysis

The following provides a comparison between the existing rule text and the final rule text.

(A) Existing Rule: Purpose. This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. Licensees subject to the provisions of § 72.182, § 72.212, § 73.20, § 73.50, and § 73.60 are exempt from § 73.1(a)(1)(i)(E) and § 73.1(a)(1)(iii).

(A) Final Rule: Purpose. This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material. Licensees subject to the provisions of § 73.20 (except for fuel cycle licensees authorized under part 70 of this chapter to receive, acquire, possess, transfer, use, or deliver for transportation formula quantities of strategic special nuclear material), § 73.50, and § 73.60 are exempt from § 73.1(a)(1)(i)(E), § 73.1(a)(1)(iii), § 73.1(a)(1)(iv), § 73.1(a)(2)(iii), § 73.1(a)(2)(iv). Licensees subject to the provisions of § 72.212 are exempt from and§ 73.1(a)(1)(iv).

(A) Change: The paragraph is modified to clarify that the DBT is designed to protect against diversion in addition to theft of special nuclear material. The exemptions are updated based on the order requirements and conforming changes to other paragraphs of this part.

(1) Existing Rule: Radiological sabotage. (i) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment:

(1) Final Rule: Radiological sabotage. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as one or more teams, attacking from one or more entry points, with the following attributes, assistance and equipment:

(1) Change: The paragraph adds new capabilities to the DBT including operation as one or more teams and attack from multiple entry points.

(1)(i)(A) Existing Rule: Well-trained (including military training and skills) and dedicated individuals,

(1)(i)(A) Final Rule: Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack,

(1)(i)(A) Change: The paragraph adds adversaries who are willing to kill or be killed and are knowledgeable about specific target selection to the DBT.

(1)(i)(B) Existing Rule: inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both,

(1)(i)(B) Final Rule: active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance,

(1)(i)(B) Change: The reference to an individual is removed and the paragraph reworded to provide flexibility in defining the scope of the inside threat.

(1)(i)(C) Existing Rule: suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy,

(1)(i)(C) Final Rule: suitable weapons, including hand-held automatic weapons, equipped with silencers and having effective long range accuracy,

(1)(i)(C) Change: The phrase "up to and including" is changed to "including" to provide flexibility in defining the range of weapons licensees must be able to defend against.

(1)(i)(D) Existing Rule: hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and

(1)(i)(D) Final Rule: hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and

(1)(i)(D) Change: This description is not revised by the final rule.

(1)(i)(E) Existing Rule: a four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment to the proximity of vital areas, and

(1)(i)(E) Final Rule: land and water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas, and

(1)(i)(E) Change: The scope of vehicles licensees must defend against is expanded to include water vehicles and a range of land vehicles beyond four-wheel drive vehicles.

(1)(ii) Existing Rule: An internal threat of an insider, including an employee (in any position), and

(1)(ii) Final Rule: An internal threat, and

(1)(ii) Change: The current rule describes the internal threat as a threat posed by an individual. The language is revised to provide flexibility in defining the scope of the internal threat without adding details that may be useful to an adversary.

(1)(iii) Existing Rule: A four-wheel drive land vehicle bomb.

(1)(iii) Final Rule: A land vehicle bomb assault, which may be coordinated with an external assault, and

(1)(iii) Change: The paragraph is updated to reflect that licensees are required to protect against a wide range of land vehicles. A new mode of attack not previously part of the DBT is added indicating that adversaries may coordinate a vehicle bomb assault with another external assault.

(1)(iv) Existing Rule: None

(1)(iv) Final Rule: A waterborne vehicle bomb assault, which may be coordinated with an external assault, and

(1)(iv) Change: The paragraph adds a new mode of attack not previously part of the DBT, that being a waterborne vehicle bomb assault. This paragraph also adds a coordinated attack concept.

(1)(v) Existing Rule: None

(1)(v) Final Rule: A cyber attack.

(1)(v) Change: Adds a cyber attack. The capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls.

(2) Existing Rule: Theft or diversion of formula quantities of strategic special nuclear material. (i) A determined, violent, external assault, attack by stealth, or deceptive actions by a small group with the following attributes, assistance, and equipment:

(2) Final Rule: Theft or diversion of formula quantities of strategic special nuclear material. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as one or more teams, attacking from one or more entry points, with the following attributes, assistance and equipment:

(2) Change: The paragraph adds new adversary capabilities to the DBT including operation as one or more teams and attack from multiple entry points.

(2)(i)(A) Existing Rule: Well-trained (including military training and skills) and dedicated individuals;

(2)(i)(A) Final Rule: Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(2)(i)(A) Change: The paragraph adds to the DBT adversaries who are willing to kill or be killed and are knowledgeable about specific target selection.

(2)(i)(B) Existing Rule: Inside assistance that may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both;

(2)(i)(B) Final Rule: Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance,

(2)(i)(B) Change: The reference to an individual is removed and the paragraph reworded to provide flexibility in defining the scope of the inside threat.

(2)(i)(C) Existing Rule: Suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy;

(2)(i)(C) Final Rule: Suitable weapons, including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy;

(2)(i)(C) Change: The phrase "up to and including" is changed to "including" to provide flexibility in defining the range of weapons licensees must be able to defend against.

(2)(i)(D) Existing Rule: Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system;

(2)(i)(D) Final Rule: Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system; and

(2)(i)(D) Change: This description is not revised by the final rule.

(2)(i)(E) Existing Rule: Land vehicles used for transporting personnel and their hand-carried equipment; and

(2)(i)(E) Final Rule: Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment.

(2)(i)(E) Change: The scope of vehicles licensees must defend against is expanded to include water vehicles and a range of land vehicles beyond four-wheel drive vehicles.

(2)(i)(F) Existing Rule: the ability to operate as two or more teams.

(2)(i)(F) Final Rule: Deleted

(2)(i)(F) Change: This requirement is included in (2)(i).

(2)(ii) Existing Rule: An individual, including an employee (in any position), and

(2)(ii) Final Rule: An internal threat,

(2)(ii) Change: The current rule describes the internal threat as a threat posed by an individual. The language is revised to provide flexibility in defining the scope of the internal threat without adding details that may be useful to an adversary.

(2)(iii) Existing Rule: (iii) A conspiracy between individuals in any position who may have:

(A) Access to and detailed knowledge of nuclear power plants or the facilities referred to in § 73.20(a), or

(B) items that could facilitate theft of special nuclear material (e.g., small tools, substitute material, false documents, etc.), or both.

(2)(iii) Final Rule: A land vehicle bomb assault, which may be coordinated with an external assault, and

(2)(iii) Change: The paragraph is updated to reflect that licensees are required to protect against a wide range of land vehicles. A new mode of attack not previously part of the DBT is added indicating that adversaries may coordinate a vehicle bomb assault with another external assault.

(2)(iv) Existing Rule: none

(2)(iv) Final Rule: A waterborne vehicle bomb assault, which may be coordinated with an external assault.

(2)(iv) Change: The paragraph would add a new mode of attack not previously part of the DBT, that being a waterborne vehicle bomb assault. This coordinated attack concept is another upgrade to the current regulation.

(2)(v) Existing Rule: none

(2)(v) Final Rule: A cyber attack.

(2)(v) Change: Adds a cyber attack. The capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls.

The Commission concludes that the amendments to § 73.1 will continue to ensure adequate protection of public health and safety and the common defense and security

by requiring the secure use and management of radioactive materials. The revised DBTs represent the largest threats against which private sector facilities must be able to defend with high assurance. The amendments to 10 CFR 73.1 reflect requirements currently in place under existing NRC regulations and orders.

V. Guidance

The NRC staff is preparing new RGs to provide detailed guidance on the revised DBT requirements in 10 CFR 73.1. These guides are intended to assist current licensees in ensuring that their security plans meet requirements in the revised rule, as well as future license applicants in the development of their security programs and plans. The new guidance incorporates the insights gained from applying the earlier guidance that was used to develop, review, and approve the site security plans that licensees put in place in response to the April 2003 orders. As such, this regulatory guidance is expected to be consistent with revised security measures at current licensees. The publication of the RGs is planned to coincide with the publication of the final rule.

1. Regulatory Guide (RG-5.69) , "Guidance for the Implementation of the Radiological Sabotage Design-Basis Threat (Safeguards)." This regulatory guide will provide guidance to the industry on the radiological sabotage DBT. RG-5.69 contains safeguards information and, therefore, is being withheld from public disclosure and distributed on a need-to-know basis to those who otherwise qualify for access.

2. Regulatory Guide (RG-5.70), "Guidance for the Implementation of the Theft or Diversion Design-Basis Threat (Classified)." This regulatory guide will provide guidance to the industry on the theft or diversion DBT. RG-5.70 contains classified information and, therefore, is withheld from public disclosure and distributed only on a need to know basis to those who otherwise qualify for access.

VI. Resolution of Petition (PRM-73-12)

The staff incorporated into this rulemaking consideration of a Petition for Rulemaking, filed by the Committee to Bridge the Gap (PRM-73-12) on July 23, 2004. The petition requested that NRC conduct a rulemaking to revise the DBT regulations (including numbers, teams, capabilities, planning, willingness to die and other characteristics of adversaries) to a level that encompasses, with a sufficient margin of safety, the terrorist capabilities demonstrated during the attacks of September 11, 2001. The petition also requested that security plans, systems, inspections, and FOF exercises be revised in accordance with the amended DBTs. Finally, the petition requested that a requirement be added to Part 73 to require licensees to construct shields against air attack (referred to as "beamhenges") so that nuclear power plants would be able to withstand an air attack from a jumbo jet similar to the September 11, 2001 attacks.

PRM-73-12 was published for public comment in the *Federal Register* on November 8, 2004 (69 FR 64690). There were 845 comments submitted on PRM-73-12, of which 528 were form letters. The staff reviewed both the petition and the comments on the petition against the supplemental DBTs to determine whether the DBTs should be revised as requested by the petitioner. Based on this review, the NRC staff determined that a number of the requested upgrades in PRM-73-12 have already been implemented in the proposed DBT rule language. The Commission partially granted the PRM-73-12 as stated in the public notice of the proposed 10 CFR 73.1 DBT rulemaking, *See,* 70 FR 67380; November 7, 2005, but deferred action on other aspects of the petition to the final rulemaking.

During the course of this rulemaking, the Commission considered whether it would be necessary to add some type of airborne threat as part of the DBTs. After careful evaluation and consideration, the Commission has chosen a two-track response to the

air threat that excludes physical security measures such as “beamhenge.” First, the Commission determined that active protection against the airborne threat requires military weapons and ordinance (i.e., ground-based air defense missiles), that rightfully belongs to the Department of Defense and thus the airborne threat is one which is beyond what a private security force can reasonably be expected to defend against. Second, licensees have been directed to implement certain mitigative measures to limit the effects of an aircraft strike. Therefore, the Commission has concluded to deny the request of the petition PRM-73-12 regarding the inclusion of the airborne threat in the DBTs, as well as beamhenge as physical security measures. More detailed information in support of the Commission’s position are provided in the comment resolutions for Factor 6: The potential for water-based and air-based threats, and Factor 9: The potential for fires, especially fires of long duration.

VII. Criminal Penalties

For the purposes of Section 223 of the Atomic Energy Act, as amended, the Commission is issuing the final rule to revise 10 CFR 73.1 under one or more sections of 161 of the Atomic Energy Act of 1954 (AEA). Criminal penalties, as they apply to regulations in Part 73 are discussed in 10 CFR 73.81.

VIII. Compatibility of Agreement State Regulations

Under the "Policy Statement on Adequacy and Compatibility of Agreement States Programs, "approved by the Commission on June 20, 1997, and published in the Federal Register (62 FR 46517; September 3, 1997), this rule is classified as compatibility "NRC." Compatibility is not required for Category "NRC" regulations. The NRC program elements in this category are those that relate directly to areas of

regulation reserved to the NRC by the AEA or the provisions of Title 10 of the Code of Federal Regulations, and although an Agreement State may not adopt program elements reserved to NRC, it may wish to inform its licensees of certain requirements via a mechanism that is consistent with the particular State's administrative procedure laws, but does not confer regulatory authority on the State.

VIX. Availability of Documents

Some documents discussed in this notice are not available to the public. The following table indicates which documents are available to the public and how they may be obtained. Public Document Room (PDR). The NRC Public Document Room is located at 11555 Rockville Pike, Rockville, Maryland 20852. Rulemaking Website (Web). The NRC's interactive rulemaking Website is located at://ruleforum.llnl.gov."MACROBUTTONHtmlResAnchorhttp://ruleforum.llnl.gov. These documents may be viewed and downloaded electronically via this Website. NRC's Electronic Reading Room (ERR). The NRC's electronic reading room is located at ="www.nrc.gov/NRC/ADAMS/index.html"MACROBUTTONHtmlResAnchorwww.nrc.gov/reading-rm.html.

Document	PDR	Web	ERR
Environmental Assessment	X	X	ML062130553
Regulatory Analysis	X	X	ML062130546
Public Comments on PRM-73-12	X	X	ML053040061
Radiological Sabotage Adversary Characteristics document	no	no	no
Theft or diversion Adversary Characteristics document	no	no	no
Technical Basis Document	no	no	no

RG 5.69 on Radiological	no	no	no
Sabotage RG -5.70 on Theft or	no	no	no
Diversion Memorandum: Status of Security-	x	x	ML041180532
Related Rulemaking Commission SRM dated	x	x	ML042360548
August 23, 2004 Memorandum: Schedule for	x	x	ML043060572
Part 73 Rulemakings Letter to Petitioner Commission SRM dated	x x	x x	ML052920150 ML053000448
October 27, 2005 Proposed Rulemaking dated	x	x	ML060090310
November 7, 2005 Public Comments on Proposed Rule	x	x	ML062130575
Commission SRM dated	x	x	ML
Final Rule Package dated	x	x	ML062130289

X. Plain Language

The Presidential memorandum dated June 1, 1998, entitled "Plain Language in Government Writing," published on June 10, 1998 (63 FR 31883) directed that the Government's documents be in plain, clear, and accessible language. The NRC requested comments on the proposed rule specifically with respect to the clarity and effectiveness of the language used. No specific comments were received on the

proposed rule related to this issue.

XI. Voluntary Consensus Standards

The National Technology Transfer and Advancement Act of 1995, Pub. L. 104-113, requires that Federal agencies use technical standards that are developed or adopted by voluntary consensus standards bodies unless using such a standard is inconsistent with applicable law or is otherwise impractical. The NRC is not aware of any voluntary consensus standard that could be used instead of the proposed Government-unique standards. The NRC will consider using a voluntary consensus standard if an appropriate standard is identified.

XII. Finding of No Significant Environmental Impact: Environmental Assessment:

Availability

The Commission has determined under the National Environmental Policy Act of 1969, as amended, and the Commission's regulations in Subpart A of 10 CFR Part 51, that this rule is not be a major Federal action significantly affecting the quality of the human environment and, therefore, an environmental impact statement is not required.

The determination of this environmental assessment is that there will be no significant offsite impact to the public from this action.

The NRC sent a copy of the environmental assessment and the proposed rule to every State Liaison Officer and requested their comments on the environmental assessment. No comments were received from the State Liaison Officer on the environmental assessment.

XIII. Paperwork Reduction Act Statement

This rule does not contain new or amended information collection requirements subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) for the near future. However, potential future changes in the threat environment may contain new or amended information collection requirements, and may impose additional burden on the licensees. Existing requirements were approved by the Office of Management and Budget, approval number 3150-0002.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

XIV. Regulatory Analysis

The Commission has prepared a regulatory analysis on this regulation. The analysis examines the costs and benefits of the alternatives considered by the Commission. The Commission requested public comment on the draft regulatory analysis. Comments raised on the draft analysis have been addressed in Section II of this document. Availability of the regulatory analysis is provided in Section VIII of this document.

XV. Regulatory Flexibility Certification

In accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), the Commission certifies that this rule does not have a significant economic impact on a substantial number of small entities. This final rule affects only the licensing and operation of nuclear power plants and Category I fuel cycle facilities. The companies

that own these plants do not fall within the scope of the definition of "small entities" set forth in the Regulatory Flexibility Act or the size standards established by the NRC (10 CFR 2.810).

XVI. Congressional Review Act

In accordance with the Congressional Review Act of 1966, NRC has determined that this action is not a “major rule” and has verified this determination with the Office of Information and Regulatory Affairs of OMB.

XVII. Backfit analysis

The NRC has determined, pursuant to the exception in 10 CFR 50.109(a)(4)(iii), that a backfit analysis is unnecessary for this final rule. Section 50.109 states 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 the security requirements 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.

List of Subjects in 10 CFR Part 73

Criminal penalties, Export, Hazardous materials transportation, Import, Nuclear materials, Nuclear power plants and reactors, Reporting and record keeping requirements, Security measures.

For the reasons set out in the preamble and under the authority of the Atomic Energy Act of 1954, as amended; the Energy Reorganization Act of 1974, as amended; and 5 U.S.C. 552 and 553; the NRC is adopting the following amendments to 10 CFR Part 73.

PART 73 – PHYSICAL PROTECTION OF PLANTS AND MATERIALS

1. The authority citation for Part 73 continues to read as follows:

AUTHORITY: Secs. 53, 161, 68 Stat. 930, 948, as amended, sec. 147, 94 Stat. 780 (42 U.S.C. 2073, 2167, 2201); sec. 201, as amended, 204, 88 Stat. 1242, as amended, 1245, sec. 1701, 106 Stat. 2951, 2952, 2953 (42 U.S.C. 5841, 5844, 2297f); sec. 1704, 112 Stat. 2750 (44 U.S.C. 3504 note). Section 73.1 also issued under secs. 135, 141, Pub. L. 97-425, 96 Stat. 2232, 2241 (42 U.S.C, 10155, 10161). Section 73.37(f) also issued under sec. 301, Pub. L. 96-295, 94 Stat. 789 (42 U.S.C. 5841 note). Section 73.57 is issued under sec. 606, Pub. L. 99-399, 100 Stat. 876 (42 U.S.C. 2169).

2. In § 73.1, paragraph (a) is revised to read as follows:

§ 73.1 Purpose and scope.

(a) *Purpose*. This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material. Licensees subject to the provisions of § 73.20 (except for fuel cycle licensees authorized under Part 70 of this chapter to receive, acquire, possess, transfer, use, or deliver for transportation formula quantities of strategic special nuclear material), § 73.50, and § 73.60 are exempt from § 73.1(a)(1)(i)(E), § 73.1(a)(1)(iii), § 73.1(a)(1)(iv), § 73.1(a)(2)(iii), and § 73.1(a)(2)(iv). Licensees subject to the provisions of § 72.212 are exempt from § 73.1(a)(1)(iv).

(1) *Radiological sabotage*. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as one or more teams, attacking from one or more entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including hand-held automatic weapons, equipped with

silencers and having effective long range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system; and

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack.

(2) *Theft or diversion of formula quantities of strategic special nuclear material*. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as one or more teams, attacking from one or more entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance;

(C) Suitable weapons, including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container

integrity or features of the safe-guards system;

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment; and

(ii) An internal threat; and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault; and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault; and

(v) A cyber attack.

* * * * * * *

Dated at Rockville, Maryland this ____ day of ___ 2006.

For the Nuclear Regulatory Commission.

Annette L Vietti-Cook,

Secretary of the Commission.

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 threats (DBTs) 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 two alternatives for consolidating the supplemental requirements put in place by the Orders with the DBT requirements in § 73.1.

The first alternative is to take no additional regulatory action ("The No Action Alternative") beyond the DBT Orders. Under this alternative, NRC would not revise the governing regulations in § 73.1 pertaining to DBTs, but would continue the status quo, which is a continuation of supplemented DBT requirements imposed through the DBT Orders.

The second alternative, which was selected, is to revise the § 73.1 DBT requirements through rulemaking. Because the DBTs involve 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 citizen 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(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 (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). Radiological sabotage specifically applies to facilities that use special nuclear material. However, current Category I facilities do not typically possess or use nuclear/radioactive materials that would constitute a radiological sabotage threat. Theft or diversion applies to facilities that receive, acquire, possess, use, or transfer formula quantities of SSNM. The DBTs are used by these licensees to form the basis for site-specific defensive strategies implemented through security plans, safeguards contingency plans, and guard training and qualification plans.

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). 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

This final rule establishes, in 10 CFR 73.1 the attributes of the DBTs the Commission concluded are appropriate. The Commission's decision was based on the analysis of intelligence information regarding the trends and capabilities of the potential adversaries and discussions with Federal, law enforcement, and intelligence community agencies. These enhanced adversary characteristics reflect the new threat environment and are described in the April 29, 2003 Orders. The resulting regulation, including the addition of the cyber threat that was not included in the proposed rule, does not constitute a backfit for this regulatory action because the approach selected for the final rule does not expand the DBTs beyond the requirements currently in place under existing NRC regulations, and Orders and Intermediate Compensatory Measures (ICM.) The ICMs (EA-02-026) directed the affected licensees to consider and address cyber safety and security vulnerabilities. Licensees were subsequently provided with a cyber security self-assessment methodology, the results of pilot studies, and a guidance document issued by the NEI to facilitate the development of site security programs, and the designated licensees have done so accordingly.

With respect to future changes to the rule or the ACDs, the Commission will comply with requirements of the Paperwork Reduction Act.

II. Analysis of Alternatives

There are two alternatives for addressing changes to the DBT requirements. Those are to take no additional regulatory action beyond the DBT Orders (No Action Alternative) and rulemaking (of which there are three variations). These alternatives are discussed below in more detail.

(a) No Action Alternative

This alternative is simply to take no additional regulatory action and**,** as a result, not revise the governing regulations in § 73.1(a) pertaining to the DBTs. This approach would continue the status quo, which is implementation of supplemented DBT requirements as imposed through the DBT Orders. While this action would save the agency resources that it would otherwise expend revising the regulation, it would leave § 73.1(a) as is, and these requirements do not reflect the DBT requirements currently in place. As such, the regulations would not be up-to-date; this situation could introduce inefficiencies into the regulatory process. Accordingly, this alternative was not selected.

(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 a change in § 2.800 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 refer to 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 reference a document within 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 is judged as being the best option that balances 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 DBTs, to make generically applicable the security requirements 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 plant 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) 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 to 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 to Other Stakeholders

The NRC staff has not identified any impacts upon other stakeholders. Public health and safety and defense and security would continue to be assured 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 stakeholdersof 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 threat in the rule text, that was implicitly addressed in the proposed rule, 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 Insititute (NEI), in order to facilitate development of site-specfic 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.

Environmental Assessment Supporting Final Rule, 10 CFR Part 73.1- Design Basis Threat

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

September 2006

UNITED STATES NUCLEAR REGULATORY COMMISSION

ENVIRONMENTAL ASSESSMENT AND FINDING OF NO SIGNIFICANT IMPACT

The Nuclear Regulatory Commission (NRC) is amending its regulations that govern the requirements pertaining to design basis threats (DBTs). This final rule makes 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 and security are adequately protected. Pursuant to Section 170E of the Atomic Energy Act (AEA), the final rule revises the DBT requirements for radiological sabotage, applicable to power reactors and Category I fuel cycle facilities, and theft or diversion of NRC-licensed Strategic Special Nuclear Material (SSNM), applicable to Category I fuel cycle facilities. Additionally, a Petition for Rulemaking (PRM-73-12), filed by the Committee to Bridge the Gap, was considered as part of this rulemaking. The NRC partially granted PRM-73-12 in the proposed rule, but deferred action on other aspects of the petition to this rulemaking. The NRC's final disposition of PRM-73-12 is contained in this document.

ENVIRONMENTAL ASSESSMENT

Identification of the Action:

The principal objective of the amendment to the DBT rule is to make generically applicable the security requirements previously imposed by the Commission's April 29, 2003, DBT Orders, which applied to existing licensees, and redefine the level of security requirements

necessary to ensure that the public health and safety and common defenses are adequately protected.

The approach in this rule maintains a level of specificity in § 73.1(a) rule language that is comparable to the current regulation, while revising DBT attributes to be consistent with the requirements imposed by the April 29, 2003 DBT Orders. The revised approach keeps certain specific additional details, which are both safeguards and classified information, in separate, non-publicly-available adversary characteristics documents.

The Congress amended the Energy Policy Act (EPAct) by adding Section 170E, which directed the Commission to initiate a rulemaking, and also directed the Commission to consider in the course of rulemaking, but not limited to, 12 factors specified in the statute. In accordance with that requirement, the Commission has considered and deliberated on the 12 factors identified in the act. The Commission has also considered, as part of rulemaking, a Petition for Rulemaking, PRM-73-12, filed by the Committee to Bridge the Gap. The petition requested that the NRC amend its regulations to upgrade the DBT regulations (in terms of numbers, teams, capabilities, planning, willingness to die and other characteristics of adversaries) to a level that encompasses, with a sufficient margin of safety, the terrorist capabilities demonstrated during the attacks of September 11, 2001. The petition also requested that security plans, systems, inspections, and force-on-force exercises be revised in accordance with the amended DBTs. Finally, the petition requested that a provision be added to Part 73 to require licensees to construct shields against air attack (referred to as “beamhenge”,) so that nuclear power plants would be able to withstand an air attack from a jumbo jet similar to the September 11, 2001 attacks. PRM 73-12 was published for public comment on November 8, 2004, (FR 68 64690.) The staff reviewed both the petition and the comments on the petition to determine whether the DBTs should be revised as the petitioner requests. Based on this

review, the NRC staff determined that PRM-73-12 should be granted in part and denied in part (see Section V of the proposed rule notice for more details.)

On November 7, 2005, a proposed rule 70 FR 67380, was published for public comment. There were 919 comments submitted on the proposed rule, of which 893 were form letters. The bulk of the comments either supported the petition or requested a stronger DBT, or proposed reconsideration of the 12 factors of the EPAct. The staff reviewed the comments on the proposed rule, and is amending its regulations that govern the requirements in 10 CFR 73.1.

The final § 73.1(a) rule language is provided below.

§ 73.1 Purpose and scope.

(a) *Purpose*. This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft or diversion of special nuclear material. Licensees subject to the provisions of § 73.20 (except for fuel cycle licensees authorized under Part 70 of this chapter to receive, acquire, possess, transfer, use, or deliver for transportation formula quantities of strategic special nuclear material), § 73.50, and § 73.60 are exempt from § 73.1(a)(1)(i)(E), § 73.1(a)(1)(iii), § 73.1(a)(1)(iv), § 73.1(a)(2)(iii), and § 73.1(a)(2)(iv). Licensees subject to the provisions of § 72.212 are exempt from § 73.1(a)(1)(iv).

(1) *Radiological sabotage*. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as

one or more teams, attacking from one or more entry points, with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack,

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance,

(C) Suitable weapons, including hand-held automatic weapons, equipped with silencers and having effective long range accuracy,

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas, and

(ii) An internal threat, and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault, and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault, and

(v) A cyber attack.

(2) *Theft or diversion of formula quantities of strategic special nuclear material*. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as one or more teams, attacking from one or more entry points, with the following at.tributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals, willing to kill or be killed, with sufficient knowledge to identify specific equipment or locations necessary for a successful attack;

(B) Active (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack) or passive (e.g., provide information), or both, knowledgeable inside assistance,

(C) Suitable weapons, including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safe-guards system;

(E) Land and water vehicles, which could be used for transporting personnel and their hand-carried equipment; and

(ii) An internal threat, and

(iii) A land vehicle bomb assault, which may be coordinated with an external assault, and

(iv) A waterborne vehicle bomb assault, which may be coordinated with an external assault.

(v) A cyber attack.

The Need for the Action:

The final action is needed to more closely align the governing regulations in § 73.1(a) pertaining to the DBTs with the DBT requirements imposed by the April 29, 2003 DBT Orders.

Environmental Impacts of the Final Action:

This environmental assessment focuses on those aspects of the § 73.1(a) rule where

the revised requirements could potentially affect the environment. The NRC has concluded that there will be no significant radiological environmental impacts associated with implementation of the final rule requirements for the following reasons:

(1) This rule change pertains only to security requirements, and specifically, would revise only the DBT requirements; it would not revise any of the Part 73 requirements which govern the response to the DBT requirements. The rule change is simply to more closely align the regulations with the DBT Orders which have already been imposed on licensees. As a result, the revised requirements does not change the DBT requirements from what is currently in place, and as such, there is no additional environmental impacts including any impact that could affect offsite radiological releases.

(2) The proposed revision to the requirements in § 73.1(a) does not result in changes to the design basis functional requirements for the structures, systems, and components (SSCs) in the facility that function to limit the release of radiological effluents during and following postulated accidents. As a result, all the SSCs associated with limiting the releases of offsite radiological effluents will continue to be able to perform their functions, and as a result, there will be no significant radiological effluent impact.

(3) The standards and requirements applicable to radiological releases and effluents are not affected by this rulemaking (nor by the Orders) and continue to apply to the SSCs affected by this rulemaking. As already discussed, implementation of the rule requirements does not result in any additional actions beyond what has already been imposed by the DBT Orders, and furthermore, the DBT Orders themselves do not result in impacts to a facility related to normal operation and any associated releases.

Because the net effect of this action is to revise the governing regulations pertaining to

the DBTs to make them more closely align to the previously imposed DBT Orders, the NRC has concluded that this action does not cause any impact on occupational exposure.

The action will not significantly increase the probability or consequences of accidents, nor result in changes being made in the types of any effluents that may be released off-site, and there would be no significant increase in occupational or public radiation exposure. The basis for this conclusion is that the proposed rule requirements does not impose new requirements beyond those already imposed through the DBT Orders and Intermediate Compensatory Measures.

With regard to potential nonradiological impacts, implementation of the rule requirements has no impact on the environment other than what has been previously discussed. The revised requirements does not affect any historic sites, does not affect nonradiological plant effluents, and causes no other environmental impact. Therefore, there are no significant nonradiological environmental impacts associated with the action.

Accordingly, the NRC staff concludes that there will be no significant environmental impacts associated with the action.

Alternatives to the Proposed Action:

As an alternative to the rulemakings described above, the NRC staff considered not taking the action (i.e., the “no-action” alternative). Not revising the DBT regulations would result in no change in current environmental impacts since the DBT requirements have already been imposed and not taking the proposed regulatory would therefore, not change the current DBT requirements. However, the no action alternative would leave the governing DBT regulations as they are, and the regulation would not reflect the actual requirements governing DBTs. The NRC staff concluded that leaving the governing DBT regulations unaligned with order requirements is not a desirable regulatory practice. In addition, the Commission directed the

staff to revise the DBT regulations in a Staff Requirements Memorandum dated August 23, 2004.

Alternative Use of Resources:

This action does not involve the use of any resources not previously considered by the NRC in its past environmental statements for issuance of operating licenses for power reactors.

Agencies and Persons Consulted:

The NRC staff developed the final rule and this environmental assessment. In accordance with its stated policy, the NRC staff provided a copy of the final rule to designated liaison officials for each state. No other agencies were consulted.

FINDING OF NO SIGNIFICANT IMPACT

On the basis of the environmental assessment, the NRC concludes that the action will not have a significant effect on the quality of the human environment. Accordingly, the NRC has determined not to prepare an environmental impact statement for the action.

Documents may be examined and/or copied for a fee, at the NRC's Public Document Room, located at One White Flint North, 11555 Rockville Pike (first floor), Rockville, Maryland 20852. Publicly available records will be accessible electronically from the Agencywide Documents Access and Management System (ADAMS) Public Library component on the NRC web site http://www.nrc.gov (Electronic Reading Room).

Dated at Rockville, Maryland, this th day of , 2006.

FOR THE NUCLEAR REGULATORY COMMISSION.

Ho Nieh, Acting Program Director,

Division of Policy and Rulemaking,
Directorate of Risk Assessment and New Projects,
Office of Nuclear Reactor Regulation.

Summary of Public Comments on the Proposed Design Basis Threat (DBT) 10 CFR 73.1

The proposed rule provided a 75-day public comment period which ended on January 23, 2006. The comment period was extended by another 30 days in response to a request from the Nuclear Energy Institute (NEI), an industry group, to allow additional time for review of the proposed rule because the comment period overlapped the year-end holidays. The extended comment period ended on February 22, 2006. A total of 919 comments were received. Sources for these include about nine hundred individuals, one county, thirteen citizen groups, one utility involved in nuclear activities, and two nuclear industry groups. The comments covered a range of issues, some of which were beyond the scope of this rulemaking in that they were specific to measures but did not relate to the adversary characteristics. The comments have been organized under three groups ; Group I: Consideration of the 12 factors in the EPAct, Group II: In Scope comments, which includes comments raising issues and concerns directly related to the contents of the DBT rule, and Group III: Out of Scope comments, which includes comments raising issues and questions that are not directly related to the DBT rule, although they are relevant to the security of nuclear facilities.

Group I: Considerations of the 12 Factors in the Energy Policy Act

The commission's considerations, public comments and responses to the public comments are provided in the *Federal Register* Notice, Section A.

Group II: In Scope of comments

The commission's considerations, public comments and responses to the public comments are provided in the *Federal Register* Notice, Section B.

1. Definition of the Design Basis Threat
2. Applicability of the Enemy of the State
3. Compliance with Administrative and Procedures Act Notice and Comment Requirements
4. Ambiguous Rule Text
5. Differentiation in Treatment of General and Specific License for ISFSI

6. Applicability of the DBTs to the New Nuclear Power Plants
7. Consideration of Uniqueness of Each Plant in application of the DBTs
8. Continued exemption of Research Reactors from the DBT requirements
9. Changes in Security Requirements to be Addressed Under Backfit Rule
10. Compliance with the Paperwork Reduction Act
11. Adequacy of the Regulatory Analysis
12. Compliance with the National Environmental Protection Agency (NEPA)
13. Issuance of Annual Report Card on Individual Licensees

Group III: Out of Scope Topics

14. Federalization of Security
15. Force-on-Force Tests of Security
16. Screening of Workers of Nuclear Power Plants
17. Self Sufficient Defense Capabilities
18. Security of Dry Cask Storage
19. Spent Fuel Pools
20. Inherent Vulnerabilities of Design

A Comments matrix has been provided in Appendix A, which references each topic with comments.