UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT
THURGOOD MARSHALL U.S. COURTHOUSE
40 FOLEY SQUARE
NEW YORK 10007

Thomas Asreen
ACTING CLERK

Date: 5/17/07

Docket **07-2052-ag**
Short Title: The State of New York v. United States Nuclear Reg
Agency Number: RIN 3152-AH60
Agency: Nuclear Regulatory Commission

Dear Counsel:

Please be advised that a petition to review an order of the United States Nuclear Regulatory Commission in the above-entitled case has been filed in this court.

A copy of the petition is enclosed herewith.

Please acknowledge receipt of the copy of the petition on the copy of this letter also enclosed and return to me.

Very truly yours,
Thomas Asreen, Acting Clerk
By: Yana Segal
Yana Segal
Deputy Clerk

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT
THURGOOD MARSHALL U.S. COURTHOUSE
40 FOLEY SQUARE
NEW YORK 10007

Thomas Asreen
ACTING CLERK

Date: 5/17/07

Docket **07-2052-ag**
Short Title: The State of New York v. United States Nuclear Reg
Agency Number: RIN 3152-AH60
Agency: Nuclear Regulatory Commission

Deputy Clerk: Yana Segal Telephone: **(212) 857-8658**

Dear Counsel:

We have today docketed a petition for review filed by The State of New York in the above referenced case as 07-2052-ag. Please note that the following number must appear on all documents related to this case which are submitted to this Court: 07-2052-ag Enclosed are a copy of our docket sheet including the caption page, and instructions regarding the filing and processing of an appeal in this Court. Also enclosed is an acknowledgment letter. **Please return the enclosed acknowledgment within ten days of the date of this letter with the following information:**

YOUR CORRECT ADDRESS, TELEPHONE NUMBER, FAX and E-MAIL: Please check the enclosed attorney listing page of the docket sheet and advise this Court of any incorrect information in writing on the enclosed acknowledgement form.
The Court will give notice or serve copies of orders to only one counsel per party (or group of collectively represented parties.) Counsel are required to designate on the attached Acknowledgement letter a lead attorney to accept all notice from this Court in this appeal, who will, in turn, be responsible for notifying any associated counsel.

CAPTION: Attached is the full caption in this matter. Please review this attachment carefully and promptly advise this Court of any discrepancies in writing on the enclosed acknowledgement form.

APPELLATE DESIGNATIONS: Please review whether your client is correctly listed as petitioner or respondent in the party listing page of the docket sheet and in the caption. Should you believe there is an error, please advise in writing on the acknowledgement form. Timely submission of the acknowledgment form will be constituted as compliance with the requirement to file a Representation Statement set forth in Rule 12(b) of the Federal Rules of Appellate Procedure.
Please read the enclosed instructions. If you have any questions with regard to this pending appeal, please call the Deputy Clerk whose name is given above.

Enclosures:

USCA Docket Sheet, including Caption Page
Instructions
Acknowledgement Form

NON-PUBLIC DOCKET FOR
Second Circuit Court of Appeals

INDIV

Court of Appeals Docket #: 07-2052-ag
Nsuit:
The State of New York v. United States Nuclear Regulatory Commission
Appeal from: Nuclear Regulatory Commission

Filed: 5/14/07

Case type information:

Agency
Petition for Review
None

Lower court information:

District: RIN 3152-AH60
Trial Judge:
MagJudge:
Date Filed:
Date order/judgement:
Date NOA filed: 5/14/2007

Fee status: Paid

Panel Assignment:

Panel:

Date of decision:

Prior cases: NONE

Current cases: NONE

Official Caption 1/

Docket No. [s] : 07-2052 -ag

The State of New York,

Petitioner,

v.

United States Nuclear Regulatory Commission, United States of America,

Respondents.

Authorized Abbreviated Caption 2/

Docket No. [s] : 07-2052 -ag

The State of New York v. United States Nuclear Regulatory Commission

---

1/ Fed. R. App. P. Rule 12 [a] and 32 [a].
2/ For use on correspondence and motions only.

United States of America
Respondent

Alberto Gonzales Esq.
[LD n]
US Dept. of Justice
950 Pennsylvania Ave., NW
Washington , DC , 20530

The State of New York
Petitioner

John J. Sipos Esq.
[LD n]
New York State Department of Law
120 Broadway
New York , NY , 10271
518-402-2251

United States Nuclear Regulatory Commission
Respondent

Karen Cyr Esq.
[n]
United States Nuclear Regulatory Commission
11555 Rockville Pike
Rockville , MD , 12224

5/14/07	Case Docketed: Petition for review of agency order on behalf of PETITIONER The State of New York, filed. [Entry date May 17 2007]
5/14/07	Copy of the United States Nuclear Regulatory Commission's final rule, filed. [Entry date May 17 2007]
5/14/07	Copy of receipt re: payment of docketing fee filed on behalf of PETITIONER The State of New York. RECEIPT #187953 [Entry date May 17 2007]
5/17/07	Served copy of petition under cover letter on respondent. [Entry date May 17 2007]

United States Court of Appeals Second Circuit
Thurgood Marshall U.S. Courthouse
40 Foley Square
New York, N.Y. 10007
(212) 857-8500

NOTICE

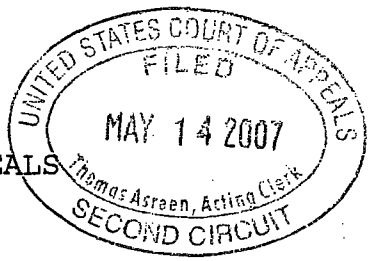
Please visit the Clerk`s Office Forms section of the Court`s website which is located at:

http://www.ca2.uscourts.gov

To download

- **Instructional Booklet: How to Appeal Your Civil Case**
- **Instructional Booklet: How to Appeal Your Criminal Case**
- **Instructional Booklet: How to Appeal Your Habeas Case**
- **Requisite Court Forms: Form C, Form D, Form C/A, Notice of Appearance, Electronic Notification Form, T-1080 Motion Information Form and many others.**

07-2052cvg



UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

----------x

THE STATE OF NEW YORK,

Petitioner,

-against-

No. _____

UNITED STATES NUCLEAR
REGULATORY COMMISSION, and

UNITED STATES OF AMERICA,

Respondents.

----------x

PETITION FOR REVIEW

Pursuant to § 189 of the Atomic Energy Act, 42 U.S.C. § 2239, 28 U.S.C. §§ 2341-2344, and Rule 15 of the Federal Rules of Appellate Procedure, the petitioner, the State of New York, by its attorney, Andrew M. Cuomo, Attorney General of the State of New York, hereby petitions this Court for review of the United States Nuclear Regulatory Commission's ("NRC") final rule amending Part 73 of Title 10 of the Code of Federal Regulations, § 73.1, entitled "Design Basis Threat." The final rule fails, among other things, to include air-based threats or air attacks

within the design basis threats for the protection of special nuclear material from radiological sabotage and the prevention of theft or diversion of nuclear material at nuclear power plants and other facilities.

The final rule and the NRC's rationale thereof were published at 72 Federal Register 12705-12727 (March 19, 2007), a copy of which is attached hereto. In the underlying rulemaking proceeding (NRC No. RIN 3150-AH60 and PRM-73-12), the NRC amended its regulations that govern the requirements pertaining to design basis threats. The final rule has been, or will be, codified at 10 C.F.R. § 73.1 and became effective on April 18, 2007.

The State contends that by failing to address relevant facts presented to it or existing in the public domain and without an adequate analysis of the underlying considerations relevant to its decision, the NRC acted arbitrarily, abused its discretion, and violated the Atomic Energy Act, the Energy Policy Act of 2005, the Administrative Procedures Act, the National Environmental Policy Act, and other applicable laws and regulations.

Venue is appropriate within the Second Circuit pursuant to 28 U.S.C. § 2343 since the State of New York resides in and maintains its principal office within the Second Circuit.

Therefore, the State respectfully requests that this Court review the NRC's determination in RIN 3150-AH60 and PRM-73-12, vacate the NRC's determination regarding the design basis threat rule, 10 C.F.R. § 73.1, remand the matter to the NRC for further consideration and review of public comments, and for any other relief that the Court may deem just and appropriate.

Dated: May 16th, 2007
Albany, New York

ANDREW M. CUOMO
Attorney General of the State of New York

BY: John J. Sipos (AW)
JOHN J. SIPOS
Assistant Attorney General
Environmental Protection Bureau
New York State Attorney General's Office
The Capital
Albany, New York 12224
Tel. (518) 402-2251
Fax (518) 473-2534
e-mail: john.sipos@oag.state.ny.us

Attorneys for Petitioner State of New York

cc: United States Nuclear Regulatory Commission
11555 Rockville Pike
Rockville, Maryland 20852-2738

Attorney General of the United States
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

********** -COMM. JOURNAL- ********** DATE MAY-22-2007 ***** TIME 17:35 *** P.01

MODE = TRANSMISSION START=MAY-22 17:34 END=MAY-22 17:35

STN NO.	COM	ABBR NO.	STATION NAME/TEL.NO.	PAGES	DURATION
001	OK	☎	92025887795	003	00:00'49"

********** - - ***** - - *********

Appendix to Petition

72 Federal Register 12705-12727 (March 19, 2007)

Concerning

Design Basis Threats

(NRC No. RIN 3150-AH60 and PRM-73-12)

rule modified existing debt refinancing eligibility language and inadvertently omitted three key words that existed prior to the final rule taking effect. This rule inserts those three words back into the debt refinancing eligibility language.

List of Subjects in 7 CFR Part 4279

Business and industry, Loan programs, Rural areas, Rural development assistance.

■ Accordingly, chapter XLII, title 7, Code of Federal Regulations, is amended as follows:

PART 4279—GUARANTEED LOANMAKING

■ 1. The authority citation for part 4279 continues to read as follows:

Authority: 5 U.S.C. 301 and 7 U.S.C. 1989.

Subpart B—Business and Industry Loans

■ 2. In § 4279.113, paragraph (r) is revised to read as follows:

§ 4279.113 Eligible loan purposes.

* * * * *

(r) To refinance outstanding debt when it is determined that the project is viable and refinancing is necessary to improve cash flow and create new or save existing jobs. Except as provided for in § 4279.108(d)(4) of this subpart, existing lender debt may be included provided that, at the time of application, the loan has been current for at least the past 12 months (unless such status is achieved by the lender forgiving the borrower's debt) and the lender is providing better rates or terms. Subordinated owner debt is not eligible under this paragraph. Unless the amount to be refinanced is owed directly to the Federal government or is federally guaranteed, the existing lender debt refinancing must be a secondary part (less than 50 percent) of the overall loan.

* * * * *

Dated: February 23, 2007.

Jackie J. Gleason,

Administrator, Rural Business—Cooperative Service.

[FR Doc. E7–4920 Filed 3–16–07; 8:45 am]

BILLING CODE 3410–XY–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 security requirements similar to those previously imposed by the Commission's April 29, 2003 DBT Orders, based upon experience and insights gained by the Commission during implementation, 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, generally applicable to power reactors and Category I fuel cycle facilities, and for 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 the final rule. The NRC's final disposition of PRM–73–12 is contained in this document.

DATES: *Effective Date:* April 18, 2007.

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
II. Analysis of Public Comments and Consideration of the 12 Factors of the Energy Policy Act of 2005
III. Summary of Specific Changes Made to the Proposed Rule as a Result of Public Comments
IV. Section by Section Analysis
V. Guidance
VI. Resolution of Petition (PRM–73–12)
VII. Criminal Penalties
VIII. Compatibility of Agreement State Regulations
IX. Availability of Documents
X. Plain Language
XI. Voluntary Consensus Standards
XII. Finding of No Significant Environmental Impact: Environmental Assessment: Availability
XIII. Paperwork Reduction Act Statement
XIV. Regulatory Analysis
XV. Regulatory Flexibility Act Certification
XVI. Backfit Analysis
XVII. Congressional Review Act

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

Following the terrorist attacks on September 11, 2001, the NRC conducted a thorough review of security practices to ensure that nuclear power plants and other licensed facilities continued to have effective security measures in place to address the changing threat environment. The NRC recognized that some elements of the DBTs required enhancement. After soliciting and receiving comments from Federal, State, and local agencies, and industry stakeholders, and reviewing 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: Augmented security forces and capabilities; increased patrols; additional security posts and physical barriers; vehicle checks at greater standoff distances; enhanced 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 general 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 (69 FR 64690; November 8, 2004). PRM–73–12 requests 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 encompasses, with a sufficient margin of safety, the terrorist capabilities evidenced by the attacks of September 11, 2001. The petition also requests 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 of this document.

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, that required the Commission to initiate a rulemaking to revise the DBTs. In addition, Section 170E also directed the Commission to consider but not be limited to, the 12 factors specified in the statute in the course of that rulemaking. 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, EPAct requirements, and the public comments on the proposed rule. The Commission has considered and deliberated on the 12 factors identified in the EPAct. The results of its consideration are set forth in Section II of this document. Additionally, the Commission specifically invited public comments on how these factors should be addressed in the rule. Many of the comments received substantively 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 against which nuclear power plants and Category I fuel cycle facilities are required to defend. 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 the DBT 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 (SGI). The technical bases for the ACDs are derived largely from intelligence information. They also contain classified or SGI 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 cleared for access.

Because 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 that 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 from about 903 individuals, one county, 13 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 because they were specific to protective 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, that includes comments raising issues and concerns directly related to the contents of the DBT rule; and Group III, Out-of-Scope comments, that includes comments raising issues and questions that are not directly related to the DBT rule, although they

are generally 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 consideration, 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 Groups 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 Threats
2. Applicability of the Enemy of the State Rule
3. Compliance with Administrative Procedure Act (APA) Notice and Comment Requirements
4. Ambiguous Rule Text
5. Differentiation in Treatment of General and Specific Licenses for ISFSI
6. Applicability of the Radiological Sabotage DBT 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 Policy Act (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, that 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 but not be limited to, the 12 factors specified in the statute in the course of the DBT rulemaking. 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. However, the EPAct did not require that the Commission explicitly include any of the 12 factors in the proposed or final rule text. The Commission carefully considered intelligence information, vulnerability assessments, other Commission-sponsored studies, and 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 groups [1] 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 and law enforcement information, the Commission has decided to explicitly include a cyber threat as an attribute 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 deferred its consideration of air-based threats to the final rule, thus undermining stakeholders' abilities to know the Commission's position on that factor. 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 but the Commission specifically sought comment on the issue in the proposed DBT rule and has remained open to changing its position. 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. The assertion about the lack of APA notice with regard to the EPAct's 12 factors is without merit. The proposed rule discussion contained, under a section designated "Proposed Regulations," (70 FR 67381) a detailed listing and clarifying discussion of the 12 factors and a specific request for public comment on "whether or how the 12 factors should be addressed in the DBT rule." (70 FR 67382).

Factor 1. The Events of September 11, 2001

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 NRC promptly reevaluated the DBTs and imposed additional requirements on licensees through orders, including the April 29, 2003 Orders on the DBTs. A number of revisions to the DBTs have resulted from consideration of the events of September 11, 2001. Those revisions include increased adversaries' willingness to kill or be killed, and the capability to operate in several different modes of attack, including multiple adversary groups, and multiple adversary entry points.

Public Comment: Several commenters specifically challenged the proposed rule's consideration of the events of September 11, 2001, expressing concern

[1] For purposes of this rule, there is no substantive difference between the terms "group" and "team" in reference to the operational capabilities of the DBT adversary force. The meaning of the term "group" is the same as the meaning of the term "team" used in the proposed rule. The term "team" was preserved in this final rule only when summarizing comments on the proposed rule or the 12 Factors of the EPAct.

that the DBT rule does not require licensees to defend against a number of attackers comparable to the number of terrorists (19) who participated in the attacks on September 11, 2001.

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 detail 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. However, 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." Consideration of seemingly inconsistent views 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

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, the Commission believes they are appropriate. 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 reflects the Commission's determination of the composite set of adversary features against which private security forces should reasonably have to defend.

The DBT rule has been amended in several significant respects to reflect the current physical, cyber, biochemical, and other terrorist threats. For example, the radiological sabotage DBT has been enhanced to reflect the requirement that the licensees have a capability to defend against attackers with the ability to operate in several modes of attack, including as multiple groups, attacking from multiple entry points. Additionally, in § 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 relates to physical threats from 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, § 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.

The Commission has also carefully considered biochemical threats both before and after the events of September 11, 2001. The previous rule already contained requirements that provided the capability of using "incapacitating agents," and that attribute has been retained in the final rule. In addition, armed responders are required to be equipped with gas masks to effectively implement the protective strategy and mitigate the effects of the incapacitating agents.

Public Comment: Although many of the public comments could generally be characterized as addressing Factor 2, only a few 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, that 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 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.

Response to Public Comment: Regarding the threat of cyber attack comment, the NRC agrees with the statement submitted by the commenter and explicitly included a cyber attack 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 of this document. In addition, the proposed 10 CFR 73.55(m), "Digital Computer and Communication Networks," that is included in the proposed rule, "Power Reactor Security Requirements," (71 FR 62664; October 26, 2006), contains proposed measures to mitigate a cyber attack.

With respect to the other comments regarding protection against explosives of considerable size and modern weaponry, as stated earlier, the details of the adversary capabilities can not be specified publicly, but the Commission believes they are appropriate. Furthermore, the land vehicle bomb assault may be coordinated with an external assault, maximizing its destructive potential.

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, because there is no theoretical limit to what attack scenarios can be conceived. Therefore, the NRC staff considers the tactics that have been observed in use, discussed, or trained for by potential adversaries. These tactics and DBT provisions are subjected 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—include cyber threat as an attribute; disagrees with the 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

The Commission's Consideration: The number of attackers and the tactics used by those attackers is now and has always been a 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 how these numbers are derived. As noted in the Commission's consideration of 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, and homeland security agencies using a variety of classified and unclassified sources. A statistical analysis was done on terrorist group size by looking at hundreds of terrorist attacks over several years, and comparing them with previous group size analyses for changes in long-term trends. Large "outlier" terrorist events, although 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 in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points." By revising the language in the rule and eliminating the reference to "several persons" and "small group," the NRC actually increased the potential flexibility of the design basis adversary. The use of multiple adversary groups is not necessarily tactically advantageous to the attacking force in all possible scenarios. In some instances, the adversary force, as simulated in Force-on-Force (FOF) exercises can, based on its analysis of the licensee's protective strategy, concentrate its force in a single group if necessary to best attack a facility. In other instances, a licensee's protective strategy may be more vulnerable to multiple groups 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, while the guidance provides sufficient specificity.

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

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 which licensees must defend against. In summary:

- NRC position: Agrees partially with the comment.
- Action: No additional action required, beyond adoption of more specific language in the final rule.

Factor 4. The Potential for Assistance in an Attack From Several Persons Employed at the Facility

The Commission's Consideration: The Commission has always considered the threat of insider assistance to be a very real and significant threat. Thus, the DBTs have long contained a provision requiring licensees to protect against insider assistance. Also, other NRC regulations contain substantial requirements for access authorization programs (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"). However, the final rule 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." Therefore, this provision suggests that this knowledge could be obtained from an insider who has such knowledge.

The insider 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.

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.

Response to Public Comment: The NRC 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.

The 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 trustworthiness. The NRC recognizes that those processes exist and provide an appropriate level of 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 established emergency response protocols. If a particular responding organization had been penetrated by an adversary insider, then that adversary would be considered an external adversary for purposes of the DBTs. The requirement that licensees protect against "A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions," as described in §§ 73.1(a)(1)(i), and 73.1(a)(2)(i), anticipates such an adversary. 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

The Commission's Consideration: The final rule contains language reflecting the potential for suicide attacks. This level of commitment has been assumed since the first DBTs were established by the NRC. Language has been added to §§ 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."

Public Comment: No public comment received.

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 attribute 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 ordnance 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 discounting the airborne threat; merely that the responsibility for actively protecting against the threat lies with other organizations 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. The deployment of ground-based air defense weapons would be a decision for the Departments of Defense, Homeland Security, Transportation and Justice, not the NRC. In addition, 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 for a commercial entity to get permission to engage. The potential for collateral damage to the surrounding community also would have to be considered. Deployment of protective measures such as no-fly zones, combat air patrols, and ground-based air defenses are undertaken by many other Federal organizations 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 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. 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.

In February 2002, the Commission, in addition to the actions of other Federal entities, 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. NRC staff conducted mock exercises to practice imminent air attack responses with each licensee. The NRC has continued to work with licensees on these issues and has inspected licensee actions to identify 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 the low likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety. 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 potential radioactive source term for off-site emergency planning basis. Nevertheless, on June 20, 2006, the NRC issued orders to appropriate power reactor licensees requiring the implementation of additional 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. This information is discussed in, "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 organizations (NRC, DHS, DOD, and FBI) in the event of a nuclear plant aircraft attack and clarified protocols for response-related interagency communication and coordination.

The final DBT contains two new provisions that account for the capability of a water-based attack, 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, intelligence community, and homeland security

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. 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.

Public Comment: Approximately 820 comments indicated that the "beamhenges" concept or similar barrier method of protection should be considered for protection against airborne attacks. As generically described by the commenters, a "beamhenge" shield is constructed out of an interlocking series of steel I-beams and cables that would be built at sufficient stand-off distances from safety-related buildings at nuclear power plants to protect against an aircraft attack. 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 the 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.

Response to Public Comment: The Commission has spent considerable time and resources considering the threat of airborne and waterborne attacks on nuclear facilities. Based on these considerations, the NRC has chosen a two-track approach to respond to these threats in order to assure adequate protection. First, the NRC has determined that active protection against the airborne threat rests with other organizations of the Federal government, such as NORTHCOM and NORAD, TSA, and FAA. The NRC will continue to test these relationships through exercises. 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 on the issue, but has rejected the concept because it believes that the mitigation measures in place are sufficient to ensure adequate protection of the public health and safety.

With respect to the waterborne attack threat, 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 (71 FR 62664; October 26, 2006) 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. In summary:

- NRC Position: Agrees with the waterborne 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

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. The Commission notes that the DBTs have been revised to specifically reflect these two considerations. First, §§ 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.

Public Comment: Refer to Factor 2.

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

The Commission's Consideration: As noted above under the discussion of Factor 4, §§ 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."

Public Comment: No public comment received.

Response to Comment: No response required.

Factor 9. The Potential for Fires, Especially Fires of Long Duration

The Commission's Consideration: The DBTs describe specific adversary characteristics against which licensees must be prepared to defend. Fires, in contrast, are not adversary characteristics, but result from a particular adversary attack. Nevertheless, the NRC considered fires resulting from several possible initiating 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. A summary of the assessment study is available in a publicly available document.

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

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 Nation's nuclear power plants, an initiative was undertaken as part of a February 2002 NRC Order. The order 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 if 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 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 of 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 off-site emergency plans such that the NRC's emergency planning basis remains valid (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

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

Public Comment: No public comment received.

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

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, following the terrorist attacks of September 11, 2001, the NRC evaluated the emergency preparedness (EP) planning basis and determined that the planning basis for nuclear power reactors remains valid. Further, the NRC issued orders requiring compensatory measures for nuclear security and safety, and observed licensee performance during security-based EP drills and exercises and security FOF exercise evaluations. Also, the NRC reviewed current public radiological protective action guidance, and discussed security-based EP issues with various stakeholders, including licensees and Federal, State and local government officials. Based on the information obtained from the reviews and evaluations, the NRC determined that EP of nuclear power plants could be enhanced. The Commission approved the communication of enhancements to EP and response actions for security-based events to power reactor licensees. NRC Bulletin 2005–02, "Emergency Preparedness and Response Actions for Security-Based Events," dated July 18, 2005, communicated enhancements in the following areas:

- Security-based emergency classification levels and emergency action levels;
- A 15 minute prompt notification to the NRC for security-based events;
- On-site protective actions to maximize personnel safety during security-based events;
- Enhanced emergency response organization augmentation; and
- Development of a security-based emergency drill and exercise program.

As of February 18, 2006, all power reactor licensees have implemented the enhancements to their EP programs with the exception of the drill and exercise program. A majority of nuclear power plant licensees indicated that adoption of the security-based EP drill and exercise program is contingent on NRC and the Department of Homeland Security (DHS) endorsement. The NRC continues to work with DHS and the Nuclear Energy Institute to develop and implement a security-based drill and exercise program at power reactor licensees. This program is being conducted in a phased approach. Tabletop drills at four power reactor sites and a facility drill were conducted successfully, and areas for improvement were identified and incorporated by the industry into draft guidelines. Over the next three years, the industry plans to conduct security-based EP drills at each power reactor licensee with an end state of the integration of security-based EP scenarios into the biennial EP exercise program.

In addition to those security-related emergency planning efforts, the NRC and DHS worked together to develop and improve EP for a terrorist attack through federal initiatives such as comprehensive review programs and integrated response planning efforts. The NRC and DHS have enhanced the coordination of integrated EP programs through evaluations of licensee and State/local/tribal response capabilities, 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 EP measures, and continued improvement in capabilities for licensees and off-site response organizations to respond to a wide spectrum of events.

Public Comment: No public comment received.

Response to Public Comment: No response required.

Factor 12. The Potential for Theft or Diversion of Nuclear Material From Such Facilities

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, as embodied in the rule text of §§ 73.1(a)(1) and in 73.1(a)(2), respectively, are the same, the ACDs and RGs differ 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 (most power reactor spent fuel is considered "self-protecting"). As stated in the response to Group III Comments No. 18 (Security of Dry Cask Storage) and 19 (Security of Spent Fuel Pools), the NRC has required that licensees take additional security and mitigating measures against a radioactive release of spent fuel.

The NRC has authorized the Duke Energy Corporation, owner and operator of the Catawba plant, to irradiate 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 Strategic Special Nuclear Material, in this case plutonium, and 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 theft and diversion standpoint at the reactor site due to its low plutonium concentration, composition, and form (size and weight). The MOX fuel consists of plutonium oxide particles dispersed in a ceramic matrix of depleted uranium oxide with a plutonium 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. The staff therefore approved the exemptions requested to these regulations, finding that they were authorized by law, and will not endanger life or property or the common defense and security, and that are otherwise in the public interest. The Commission later approved this determination in an adjudicatory order issued on June 20, 2005. Duke Energy Corporation (Catawba Nuclear Station, Units 1 and 2), CLI–05–014, 61 NRC 359,363 (2005).

Furthermore, transportation of the MOX fuel assemblies to Catawba will be done by the Department of Energy's (DOE's) Office of Secure Transportation, that 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.

Public Comment: No public comment received.

Response to Public Comment: No response required.

Section B

Group II. In Scope Comments

1. Defining the "Design Basis Threat"

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." 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.

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 would unnecessarily limit the Commission's judgment. This judgment is guided by the Commission's considerable expertise in nuclear security matters, developed over the course of 30 years of experience regulating the physical protection of nuclear facilities.

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 these measures. As it has stated publicly many times, the Commission is confident that neither measure is necessary or even prudent. 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 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 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 also documented when the Commission originally studied the issue

in 1976 in a report to Congress titled the "Security Agency Study."

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 the nuclear industry. 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. In addition, the Commission previously decided not to require licensees to defend against attacks by "Enemies of the State" as defined by 10 CFR 50.13.

However, these limitations on weapons and defensive systems available to private security forces do not 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, the DHS, 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 power reactor licensees' security programs to 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, on-site security 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 in response to both DBT 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 organizations 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, these 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.

However, the DBTs are not defined by cost considerations, as suggested by several commenters. The rule text set forth at § 73.1 represents the largest adversary against which the Commission believes private security forces can reasonably be expected to defend. Thus, when the DBT rule is used by licensees to design their site specific protective strategies, the Commission is thereby provided with reasonable assurance that the public health and safety and common defense and security are adequately protected. The Commission agrees with the commenters that it may not legally consider economic factors in determining the level of adequate protection of public health and safety and common defense and security (Union of Concerned Scientists v. NRC, 824 F.2d 108, 117118 (D.C. Cir. 1987)), and it did not do so in deciding what level of protection it considers to be adequate in this rulemaking. Rather, as the Commission has clearly set forth above, the requirements in the DBT rule are determined by the Commission's consideration of the staff's threat assessments based on coordination with law enforcement, intelligence, and homeland security agencies, the Commission's considerable experience in these matters, and the legal limitations on security forces available to licensees. In contrast, the Commission's determination of specific aspects of implementation of and compliance with the DBT rule, as described in the ACDs and regulatory guidance, may involve consideration, along with other factors, of the relative costs of various methods of implementing particular requirements of the DBTs. In summary:

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

2. Applicability of the Enemy of the State Rule

Public Comment: Several commenters also suggested that the proposed rule does not clearly distinguish between a threat posed by an "enemy of the state" excluded by 10 CFR 50.13, and threats covered by 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-Qaeda like terrorist organization" as an "enemy of the state" notwithstanding the Commission's statements in the vehicle bomb rulemaking, that described the characteristics of an "enemy of the state," that seemingly would have included organization like an Al-Qaeda.

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, and that any escalation of this adversary would be inconsistent with 10 CFR 50.13. These threats are properly the responsibility of the national defense establishment and other security agencies.

Response to Public Comment: The enemy of the state rule, 10 CFR 50.13, was promulgated in 1967 amid concerns that Cuba might launch attacks against nuclear power plants in Florida. That rule (32 FR 13455; September 26, 1967) was primarily intended to make clear that privately-owned nuclear facilities were not responsible for defending against attacks that typically could only be carried out by foreign military organizations. 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 is considered to be "beyond-DBT," regardless of whether it would or would not be deemed an "enemy of the state." The Commission disagrees that any extension of the DBTs automatically conflicts with 10 CFR 50.13. The Commission may revise 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 Procedure Act (APA) Notice and Comment Requirements

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 with certain parties. Also, because 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 did 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 the ACDs and RGs 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.

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 (70 FR 67380, 67382; November 7, 2005), the Commission has carefully balanced the public interest in knowing 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. 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 was necessary to understand or to comment on the proposed DBT rule.

The ACDs and RGs are guidance documents containing 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 (5 U.S.C. 553(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.

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 was 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 NRC 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 the appropriate clearance and a specific need to know the information in order to assist licensees in planning and designing protective strategies capable of defending against the DBTs. The NRC also shared those documents 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 SGI ACDs and RGs.

The NRC 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. The Commission reiterates that no SGI or classified information was 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 Office of the Federal Register regulations. In summary:

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

4. Ambiguous Rule Text

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."

Response to Public Comment: Though the Commission does not necessarily agree that the phrase "capable of operating as one or more teams" is ambiguous, in the final rule, it has nevertheless modified this language to be clear that licensees are required to defend against multiple modes of attack, including both a single group as well as multiple groups. Notably, the prior radiological sabotage DBT rule did not contain language requiring licensees to defend against multiple groups of adversaries, as specified in the theft or diversion DBT. The final rule adds a requirement to the radiological sabotage DBT that licensees protect against an adversary "capable of operating in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points," and the theft or diversion DBT has been revised for consistency. The rule therefore 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 groups and/or individuals. Neither a protective strategy that is only capable of defending against a single group nor one that is only capable of defending against a number of smaller groups would meet the requirements of the rule. The revision of this language does not, however, change the scope of this provision as originally intended by the Commission in the proposed rule. The purpose of the change is merely to provide the clearest possible articulation of the rule's requirements. In summary:

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

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

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, especially 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.

Response to Public Comment: The commenter is correct in noting that specifically-licensed and generally-licensed ISFSIs are treated differently in the current regulations. 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 excepted from certain specific requirements contained in the DBT. Ultimately, these discrepancies have no effect on the security of the facilities because 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. However, the NRC is currently considering future rulemakings to align the generally-licensed and specifically-licensed ISFSI requirements and to evaluate the application of the DBT. In summary:

- NRC position: Agrees with the comments.
- Action: No action required as part of this rulemaking.

6. Applicability of the Radiological Sabotage DBT to New Nuclear Power Plants

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.

Response to Public Comment: The NRC agrees with the commenters that the radiological sabotage DBT should be uniformly applicable to new and currently operating nuclear power plants. In fact, the NRC did not propose different radiological sabotage 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 their license application package. In summary:

- NRC position: Agrees with the comments.
- Action: No action required as part of this rulemaking.

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

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

Response to Public Comment: The DBT rule 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 each facility must have its own specific requirements. Site-specific requirements are taken into account by licensees during development of 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 FOF 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 SGI 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

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.

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) through (e) and 73.67. These regulations do not require licensees to protect against either the radiological sabotage or the theft or diversion DBT. Under 10 CFR 73.60, non-power reactor licensees who possess or use 5 kilograms or greater of HEU are exempt from the requirements in 10 CFR 73.60(a) through (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 3 feet from any accessible surface without intervening shielding.

It should also be noted that most RTRs possess limited quantities of nuclear 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/or procedures that 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 detection and response to unauthorized activities. In general, these programs include access control to the facilities, observation of activities within the facilities, and alarms or other devices to detect unauthorized presence. RTRs also have emergency plans in place 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 intend 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

Public Comment: One commentator stated that the Backfit Rule requires that the NRC perform a backfit analysis for changes in regulatory position. The commenter observed 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, but that such a determination should be supported by a documented evaluation and the proposed rulemaking does not provide such an evaluation, and each future change to the ACDs and RGs will require a separate backfit analysis.

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; November 7, 2005), the NRC has determined, pursuant to the exception in 10 CFR 50.109(a)(4)(iii) and 10 CFR 70.76(a)(4)(iv), that a backfit analysis is unnecessary for this rule. Sections 50.109 and 70.76(a)(4)(iv) state, in pertinent part, that a backfit analysis is not required if the Commission finds and declares with appropriate documented evaluation for its finding that a "regulatory action involves defining or redefining what level of protection to the public health and safety or common defense and security should be regarded as adequate." 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 similar to those 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 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

Public Comment: Several commenters stated that the Paperwork Reduction Act is circumvented by this approach. The commenters assert that 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 (70 FR 67380; November 7, 2005) states that: "This proposed rule does not contain new or amended information collection requirements subject to the Paperwork Reduction Act of 1995." 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.

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 certain details and guidance related to such threat characteristics. This approach has been adopted because the ACDs and RGs contain SGI 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 SGI 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 with the previous DBTs in § 73.1(a), and does not impose additional burden for the current 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) that supplemented the DBT, also 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.The burden for future licensees will be covered under 10 CFR Part 52 (3150–0151). In summary:

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

11. Adequacy of the Regulatory Analysis

Public Comment: A commenter stated that 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.

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 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 because 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 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. 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 threat environment may effect the ACDs and RGs, and could possibly effect 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 on the licensees. In those 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 Policy Act (NEPA)

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.

Response to Public Comment: The Commission disagrees that this rule 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 NRC prepared an environmental assessment (EA) for the proposed rule (70 FR 67387; November 7, 2005) 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. NEPA (40 CFR 1508.8(b)) only requires that the Commission consider the "reasonably foreseeable" environmental effects of its actions in determining whether an EIS is necessary. Effects that are remote, speculative, or embody the worst-case outcome of a particular action do not require an EIS.[2] In this instance, the consequences of a terrorist attack cannot be said to be "an effect" of this rule, and analyzing the effects of a terrorist attack

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

would be speculative at best. NEPA does not require such an 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 clear how publishing an EIS for public comment would result in the disclosure of additional information because NEPA does not provide any other mechanism how additional information on a proposed rule could be obtained by commenters; the APA notice and comment process provides ample opportunity to comment and provide pertinent information on the proposed rules. Nor does a request 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 need to 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. In summary:

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

13. Issuance of Annual Report Card on Individual Licensees

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.

Response to Public Comment: The NRC partially agrees with the statements submitted by the commenter. 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 detailed results of security-related drills and exercises are, and will remain, protected as SGI because this information can provide insights to potential adversaries in planning of attacks. The Commission recently submitted the first set of these reports to Congress. The unclassified version of the annual report to the Congress is publicly available, and posted on the NRC's website. 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. Under the revised policy, 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 as part of this rulemaking.

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 relevant to the DBT rulemaking. The DBT rule identifies general threat characteristics, but does not require specific protective strategies and security measures to defend against and thwart attacks. Accordingly, the following comments are deemed outside the scope of this rule. However, relevant information is provided as background material to facilitate a better understanding of the existing security measures in place and planned for the future, and to answer the underlying questions and issues raised in the following public comments.

14. Federalization of Security

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 that the Federal government should either take over the security of the plant and/or integrate the response from local, State, and Federal government resources.

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, "Security Agency Study," (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, and have high retention rates. 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, that could diminish nuclear safety.

The change would serve to increase the Federal budget needlessly. Presumably, given the enhancement in the security threat against which the guard force would be required to defend, 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. Presumably, the NRC would have to assume the responsibility for establishment of new security barriers and communications capabilities at the nuclear facilities that 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" when needed. 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

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.

Response to Public Comment: The Commission disagrees with the 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 reflected in the orders issued by the Commission on April 29, 2003. After 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. 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 documenting 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

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.

Response to Public Comment: The Commission agrees with the comment to the extent that the NRC does regulate the screening of both permanent and temporary workers with unescorted access to the protected area. The DBT rule does not regulate or oversee specific programs. Instead, it defines the general threat against which 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 be noted that the NRC requires licensees to have an access authorization program that meets NRC requirements. 10 CFR 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. Those requirements 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

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.

Response to Public Comment: The Commission disagrees with the comment. The capabilities of off-site 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, led by the DHS, 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 resulted in identifying 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. A number of Federal agencies participated in 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

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.

Response to Public Comment: The Commission disagrees with the commenters' statements. In addition, requirements related to the security of dry cask storage are beyond the scope of this rulemaking. 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 implement 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

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.

Response to Public Comment: Security program requirements are the 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 enhanced its requirements, and licensees have increased their resources to improve security 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. As a result of the supplemented DBT, the security of spent fuel pools has been enhanced at operating power reactors.

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, the NRC provided power reactor licensees additional guidance in February 2005 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. Mitigating measures that are being or have been established include those specifically recommended in the NAS study regarding fuel distribution and enhanced cooling capabilities.

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. In summary:

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

20. Inherent Design Problems That Make Power Reactors Vulnerable

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. The commenter further related the documentation of concerns of vulnerabilities regarding inherent design problems through numerous petitions and allegations to the NRC.

Response to Public Comment: The Commission disagrees with the commenter's statement that the present DBTs ignore vulnerabilities inherent in the design of nuclear facilities. The Commission has high assurance that the designs of currently operating reactors are safe, and provide adequate security protection. Moreover, the notion of "inherent design vulnerabilities" of nuclear facilities is beyond the scope of this rule, since the DBTs do not specify specific protective measures, such as design features. However, plant specific vulnerabilities are considered during the process of target set development and are utilized during force-on-force testing to assure the licensee is capable of defending the plant. In addition, the NRC is undertaking several separate rulemakings related to this issue. For instance, the Commission has proposed a rule that would amend its regulations related to security requirements for power reactors (71 FR 62664; October 26, 2006). Also, the Commission is considering issuing a proposed rule that would require applicants to assess specific design features that would be incorporated into the final design to support overall security effectiveness of nuclear power plants.

With respect to the commenter's statement on the exemptions from certain safety regulations (e.g., Appendix R fire protection standards), the NRC staff believes that the comment is out of scope of this rulemaking. However, a response to the issue raised in this question is in order. To that end, the following information is provided as background information.

Plants licensed to operate before January 1, 1979, must comply with fire protection requirements as specified in 10 CFR 50.48(b) that backfit paragraphs III.G, J and O of Appendix R. Plants licensed to operate after January 1, 1979, must comply with the approved fire protection program incorporated into their operating license. When the Commission promulgated 10 CFR Part 50, Appendix R, the Commission recognized that there would be plant specific conditions and configurations where strict compliance with the prescriptive features specified in Appendix R would not significantly enhance the level of fire safety already provided by the licensee. Therefore, in certain cases, where the licensee could demonstrate an equivalent level of fire safety that satisfied the underlying purpose of the rule, the licensee could apply for a specific exemption from Appendix R. Thus, the exemption process allowed through 10 CFR 50.12 provides a means of allowing licensees to meet Appendix R through alternate means.

The NRC has granted and continues to grant exemptions when a licensee meets the criteria of 10 CFR 50.12 and demonstrates that the alternate means provide an adequate level of fire safety. The NRC believes that individual fire protection exemptions have had a small impact on plant risk.

Regarding the commenter's statement concerning the petitions and allegations documented and submitted to the NRC, the NRC is currently preparing responses to those that have been received.

- NRC Position: Disagrees with the comment that the present DBTs ignore vulnerabilities inherent in the design of nuclear facilities.
- Action: No action is required with respect to this DBT rulemaking. However, the NRC will provide proper responses to the petitions and allegations that have been received.

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

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

The previous DBT requirements in 10 CFR 73.1 did not specifically include the threat of a cyber attack. However, a cyber attack capability was implied in the proposed 10 CFR 73.1 issued for public comment in the **Federal Register** on November 7, 2005 (70 FR 67380). Under Section 651(a)(2) of the EPAct of 2005, Congress also directed NRC to consider making an "assessment of physical, cyber, biochemical, and other terrorist threats" when developing the revised rule, and the NRC specifically asked for public comment on whether this and a number of other aspects should be included in the DBT. One commenter specifically referred to the need for the DBT rule to contain requirements pertaining to cyber attack capabilities.

The NRC has historically required licensees to evaluate cyber vulnerabilities. In February 2002, licensees subject to the DBTs were directed by ICM Order (EA-02-026) to consider and address cyber safety and security vulnerabilities. In April 2003, NRC Orders (EA-03-086 and EA-03-087) that supplemented the DBTs contained language concerning the threat of a cyber attack. 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, to facilitate development of site cyber security programs.

The February 2003, U.S. National Strategy to Secure Cyberspace suggests that the cyber threat 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," that is included in the proposed rule on power reactor security requirements (71 FR 62664; October 26, 2006), and the requirements of the EPAct of 2005, the Commission has decided to include a cyber attack as an element of the DBT.

IV. Section-by-Section Analysis

The following provides a comparison between the previous rule text and the final rule text in 10 CFR 73.1.

(a) Previous 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 § 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)(i) Previous 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)(i) 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 in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points, with the following attributes, assistance and equipment:

(1)(i) Change: The paragraph adds new capabilities to the DBT including operation in multiple modes of attack. The language in the final rule was modified to provide specificity that licensees are required to maintain the capability to protect against several modes, and that a physical security plan only capable of defending against one of the prescribed modes would not satisfy the requirements of the rule.

(1)(i)(A) Previous 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) Previous 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) Previous 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) Previous 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) Previous 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) Previous 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.

(1)(iii) Previous 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 regulations is added indicating that adversaries may coordinate a vehicle bomb assault with another external assault.

(1)(iv) Previous 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) Previous 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)(i) Previous 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)(i) 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 in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate entry points, with the following attributes, assistance and equipment:

(2)(i) Change: The paragraph adds new adversary capabilities to the DBT including operation in multiple modes of attack. The language in the final rule was modified to provide specificity that

licensees are required to maintain the capability to protect against several modes, and that a physical security plan only capable of defending against one of the prescribed modes would not satisfy the requirements of the rule.

(2)(i)(A) Previous 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) Previous 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) Previous 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) Previous 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) Previous 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) Previous 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) Previous 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.

(2)(iii) Previous Rule: 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) Previous 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) Previous 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 regulatory guides (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 SGI 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 consideration of a petition for rulemaking into this rulemaking filed by the Committee to Bridge the Gap (PRM–73–12) on July 23, 2004. The petition requests 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 requests that security plans, systems, inspections, and FOF exercises be revised in accordance with the amended DBTs. Finally, the petition requests 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 if the DBTs should be revised as requested by the petitioner. Based on this review, the NRC staff determined that a number of the proposed revisions in PRM–73–12 had already been set forth in the proposed DBT rule language. The NRC partially granted 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, particularly with respect to its consideration of the airborne threat, to the final rulemaking.

During the course of this rulemaking, the Commission considered if 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 belong to the Department of Defense. 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 denied 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 is 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 Sections of 161b, 161i, or 161o 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.

IX. 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.* These documents may be viewed and downloaded electronically via this Web site. *NRC's Electronic Reading Room (ERR).* The NRC's electronic reading room is located at *http://www.nrc.gov/reading-rm.html.*

Document	PDR	Web	ERR
Environmental Assessment	X	X	ML070530261
Regulatory Analysis	X	X	ML070530193
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 Sabotage	no	no	no
RG -5.70 on Theft or Diversion	no	no	no
Memorandum: Status of Security-Related Rulemaking	X	X	ML041180532
Commission SRM dated August 23, 2004			ML042360548
Memorandum: Schedule for Part 73 Rulemakings	X	X	ML043060572
Letter to Petitioner	X	X	ML052920150
Commission SRM dated October 27, 2005	X	X	ML053000448
Proposed Rulemaking dated November 7, 2005	X	X	ML060090310
Public Comments on Proposed Rule	X	X	ML062130575
Commission SRM dated January 29, 2007	X	X	ML070290286
Final Rulemaking	X	X	ML070520692

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 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 off-site 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 final rule does not contain new or amended information collection requirements and, therefore is not subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). Existing information collection requirements were approved by the Office of Management and Budget, approval number 3150–0002. The burden for all future licensees will be covered under 10 CFR Part 52 (3150–0151) as part of the combined operator license applications.

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 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

Under 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. Backfit Analysis

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

XVII. Congressional Review Act

Under the Congressional Review Act of 1996, 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.

List of Subjects in 10 CFR Part 73

Criminal penalties, Export, Hazardous materials transportation, Import, Nuclear materials, Nuclear power plants and reactors, Reporting and recordkeeping requirements, and 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 in each of the following modes: A single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or more individuals attacking through multiple entry points, or individuals attacking through separate 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 in each of the following modes: a single group attacking through one entry point, multiple groups attacking through multiple entry points, a combination of one or more groups and one or individuals attacking through multiple entry points, or individuals attacking through separate 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 13th day of March 2007.

For the Nuclear Regulatory Commission.

Annette L. Vietti-Cook,

Secretary of the Commission.

[FR Doc. 07–1317 Filed 3–16–07; 8:45 am]

BILLING CODE 7590–01–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Part 39

[Docket No. FAA–2006–25085; Directorate Identifier 2006–SW–02–AD; Amendment 39–14996; AD 2007–06–15]

RIN 2120–AA64

Airworthiness Directives; Eurocopter France Model AS350B, AS350B1, AS350B2, AS350B3, AS350BA, AS350C, AS350D, and AS350D1 Helicopters

AGENCY: Federal Aviation Administration, DOT.

ACTION: Final rule.

SUMMARY: This amendment adopts a new airworthiness directive (AD) for the specified Eurocopter France (Eurocopter) model helicopters that requires replacing a certain hydraulic drive belt (drive belt). Also required is reducing the lubrication time interval for a certain hydraulic pump drive shaft (drive shaft). This amendment is prompted by in-flight failures of the drive belt and the drive shaft. The actions specified by this AD are intended to prevent in-flight failure of the drive belt or drive shaft, loss of hydraulic power to the flight control system, and subsequent loss of control of the helicopter.

DATES: Effective April 23, 2007.

ADDRESSES: You may get the service information identified in this AD from American Eurocopter Corporation, 2701 Forum Drive, Grand Prairie, Texas 75053–4005, telephone (972) 641–3460, fax (972) 641–3527.

Examining the Docket: You may examine the docket that contains this AD, any comments, and other information on the Internet at *http://dms.dot.gov*, or at the Docket Management System (DMS), U.S. Department of Transportation, 400 Seventh Street, SW., Room PL–401, on the plaza level of the Nassif Building, Washington, DC.

FOR FURTHER INFORMATION CONTACT: Gary Roach, Aviation Safety Engineer, FAA, Rotorcraft Directorate, Regulations and Guidance Group, Fort Worth, Texas 76193–0111, telephone (817) 222–5130, fax (817) 222–5961.

SUPPLEMENTARY INFORMATION: A proposal to amend 14 CFR part 39 to include an AD for the specified model helicopters was published in the **Federal Register** on June 30, 2006 (71 FR 37515). That action proposed to require the following:

- At or before the next 500-hour time-in-service (TIS) inspection, replacing the drive belt with an airworthy drive belt that is not included in the applicability of this AD, and
- Within 110 hours TIS or at the next scheduled lubrication interval for the drive shaft splines, and thereafter at intervals not to exceed 110 hours TIS or 6 months, whichever occurs first, lubricating the drive shaft splines.

Eurocopter has issued the following:

- Service Bulletin No. 63.00.08, dated May 27, 2002, which specifies installing a poly-v type drive belt on the driving hydraulic pump; and
- Service Bulletin No. 29.00.04, Revision 1, dated January 27, 2004, which specifies reducing the lubrication

From: John Sipos
To: Library, Albany
Date: Mon, May 14, 2007 10:26 AM
Subject: federal register

would you please send me a pdf copy of the actual federal register notice as follows (not the Westlaw /Lexis versions, which I have)

at 72 Federal Register 12705-12727, 12726 - 12727 (March 19, 2007),

CONFIDENTIAL/PRIVILEGED/FOIL EXEMPT

John J. Sipos
Assistant Attorney General
telephone: [518] 402-2251
fax: [518] 473-2534