UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SECRETARY

January 29, 2007

COMMISSION VOTING RECORD

DECISION ITEM: SECY-06-0219

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

The Commission (with Chairman Klein and Commissioners McGaffigan, Merrifield, and Lyons agreeing) approved the final rule as noted in an Affirmation Session and recorded in the Staff Requirements Memorandum (SRM) of January 29, 2007. Commissioner Jaczko approved in part and disapproved in part.

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Commission.

Annette L. Vietti-Cook
Secretary of the Commission

Attachments:
1. Voting Summary
2. Commissioner Vote Sheets

cc: Chairman Klein
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons
OGC
EDO
PDR

VOTING SUMMARY - SECY-06-0219

RECORDED VOTES

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIP	COMMENTS	DATE
CHRM. KLEIN	X				X	12/12/06
COMR. McGAFFIGAN	X				X	11/13/06
COMR. MERRIFIELD	X				X	12/4/06
COMR. JACZKO	X	X			X	12/13/06
COMR. LYONS	X				X	11/28/06

COMMENT RESOLUTION

In their vote sheets, Chairman Klein and Commissioners McGaffigan, Merrifield, and Lyons approved the final rule. Commissioner Jaczko approved in part and disapproved in part. Subsequently, the Commission affirmed the final rule as noted in an Affirmation Session and reflected in the SRM issued on January 29, 2007.

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: CHAIRMAN KLEIN

SUBJECT: **SECY-06-0219 - FINAL RULEMAKING TO REVISE 10 CFR 73.1, DESIGN BASIS THREAT (DBT) REQUIREMENTS**

Approved xx w/edits & comments Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below___ Attached xx None ___

SIGNATURE

Dec 12, 2006

DATE

Entered on "STARS" Yes ✓ No ___

Chairman Klein's Comments on SECY-06-0219

I approve the publication of the final rule for 10 CFR 73.1, Design Basis Threat Requirements, as well as the closure of the Petition for Rulemaking (PRM) -73-12 subject to the attached edits. I believe that the final rule package reflects sound analyses of the issues presented, including the Commission's obligations under Section 651 of the Energy Policy Act of 2005 and the public comments on those and other matters. In particular, I fully support the inclusion of the threat of cyber attack as an explicit element of the DBTs. I am pleased that the Commission is now poised to promulgate updated generic regulatory requirements that reflect appropriate consideration of intelligence information, prior orders and insights from their implementation.

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 who operate as one or more teams, attacking from one or more 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 ~~includes~~ 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

- 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 ~~DBT~~ 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 safeguards information that cannot be publicly disclosed. The NRC believes that the DBTs should be uniformly applicable to all comparable nuclear facilities and will continue to ensure adequate protection of public health and safety and the common defense and security by requiring the secure use and management of radioactive materials. In summary:

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

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

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER MCGAFFIGAN

SUBJECT: **SECY-06-0219 - FINAL RULEMAKING TO REVISE 10 CFR 73.1, DESIGN BASIS THREAT (DBT) REQUIREMENTS**

Approved X Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below___ Attached X None ___

Approved subject to attached edits and comments.

Edward McGaffigan Jr.

SIGNATURE

November 13, 2006

DATE

Entered on "STARS" Yes X No ___

Commissioner McGaffigan's Comments on SECY-06-0219

I approve the final rule amending the 10 CFR 73.1 Design Basis Threat (DBT) requirements. The final rule appropriately addresses the Commission's April 29, 2003 DBT Orders and statutory obligations contained in Section 651 of the Energy Policy Act (EPAct). I commend the staff for a well reasoned and organized final rule that properly reflects the importance of security at the nation's nuclear facilities and takes into account the changing threat environment based upon a thorough analysis of relevant intelligence information.

In particular, the Staff has properly considered the twelve factors set forth in Section 170E of the Atomic Energy Act, as amended by Section 651(a) of the EPAct, modifying the rule where appropriate. Finally, I believe that the inclusion of a threat of cyber attack as an explicit attribute of the DBTs is both appropriate and necessary.

Edward McGaffigan Jr. 11/13/06

Edward McGaffigan, Jr. **(Date)**

characterized as addressing Factor 2, only ~~several~~ 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 XXX (3150-AG-63)], 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 they are indeed substantial. 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 bases the DBT adversary tactics on those 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

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 because 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.

nations

As part of a larger NRC effort to enhance the safety and security of the Nations nuclear power plants, an initiative was undertaken as part of a February 2002 NRC order. The order 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 offsite emergency plans such that the NRC's emergency planning basis remains valid (*See,* Key Radiological Protection Mitigation Strategies Order, 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

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 ~~threats that it considers to be~~ 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, onsite 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, *See,* Union of Concerned Scientists v. NRC, 824 F.2d 108, 117-118 (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 ~~as defined 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 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. *See*, 32 FR 13455; September 26, 1967. By contrast, the DBT rule does not focus on the identity, sponsorship, or nationality of the adversaries. Instead, it affirmatively defines a range of attacks and capabilities against which nuclear power plants and Category I fuel cycle facilities must be prepared to defend. An adversary force that falls outside of the range of attacks against which nuclear facilities are reasonably expected to defend are considered to be "beyond-DBT," ~~but not necessarily~~ regardless of whether they 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

access to the classified and safeguards-information 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. ~~Unfortunately, language in a *Federal Register* document granting NEI's request for a 30-day extension of the comment period could be read to suggest otherwise. *See*, 71 FR 3791; January 24, 2006.~~ The NRC shared the draft ACDs and RGs with NEI and licensees because licensees (unlike other stakeholders) need that guidance in order to develop licensee protective strategies, as is stated in the *Federal Register* document. ~~The NRC also shared these documents to get specific comments on the RGs and the ACDs that the NRC~~ is producing in ~~parallel with the r~~ule. The ACDs or RGs were not needed to comment on the rule itself. ~~The NRC's decision to extend the public comment period at the same time that it made classified and SGI guidance documents available admittedly caused some confusion~~ on this point. and were provided to NEI + licens for a purpo independen of comment on the rul

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

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

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

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 ~~for protecting against the~~ 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.

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

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 safeguards or classified information that cannot be disclosed in the public domain and would be useful to potential adversaries. This approach is not a circumvention of the Paperwork Reduction Act, but reflects the inherent dichotomy of the DBT rulemaking in trying to reach a balance between the needs for meaningful public participation and the requirement to protect safeguards and classified information, where public disclosure of specific attributes or details of security designs or protective measures would have the potential of making them ineffective.

The statement, "This proposed rule does not contain new or amended information collection.... Act of 1995," is accurate. The final rule consolidates the supplemental requirements put in place by the orders with the previous DBTs in § 73.1(a), and does not impose additional burden for the licensees even though the rule contains a cyber threat as an additional attribute of the threat. This is because the licensees subject to the DBTs were directed by the Interim Compensatory Measures (ICM) order (EA-02-026) to consider and address cyber safety and security vulnerabilities. In April 2003, the Orders (EA-03-086) and (EA-03-087) 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.

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

and Reg Guide

- 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 proposed DBT amendments would not require existing licensees to make additional changes to their current NRC-approved security plans. This premise was correct then and is correct even now because a cyber threat is explicitly included as an attribute of the final rule. Even though the regulatory

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

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, [Power Reactor Security Requirements, 71 FR XXX (3150-AG-63)], 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)~~ (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)~~ (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~~) (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) 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) Final Rule: Radiological sabotage. (i) A determined violent external assault, attack by stealth, or deceptive actions, including diversionary actions, by an adversary force capable of operating as one or more teams, attacking from one or more entry points, with the following attributes, assistance and equipment:

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

Commissioner McGaffigan's Additional Comments on SECY-06-0219

The Commission's final action on this rule will disappoint some organizations (Committee to Bridge the Gap, Nuclear Information and Resource Service, Public Citizen, and the Union of Concerned Scientists). I did not have the chance to meet with them, as they requested in a December 11, 2006 letter, because of my ongoing health issues.

However, I would like to say why I agree with the staff on both points raised in their letter.

First, on the lack of inclusion of attacks using commercial aircraft in the design basis threat (DBT). Apparently, everyone including the four groups is now in agreement that the active defenses needed to defend these sites against that threat (fighter planes and surface-to-air missiles) are absolutely inappropriate for the security forces guarding our 64 reactor sites. But the four groups would still require passive defenses, such as "beamhenges." In some sense, "beamhenges" do not belong in this rule simply on procedural grounds. This rule sets the capabilities of an attacking force against which licensees with their own security resources shall be capable of defending with high assurance (per 10 CFR 73.55). It is not about passive defenses, which could be considered again in the 10 CFR 73.55, et. al. rulemaking for which the Commission has extended this comment period. However, the "beamhenge" concept also fails substantively. Today the NRC has in place measures to prevent public health and safety impacts of a terrorist attack using aircraft that go far beyond any other area of our critical infrastructure. In addition to all the measures the Department of Homeland Security and other agencies have put in place to make such attacks extremely improbable (air marshals, hardened cockpit doors, passenger searches, etc.), NRC has entered into a Memorandum of Understanding with NORAD/ NORTHCOM to provide real-time information to potentially impacted sites of any aircraft diversion. NRC, using the insights from our research program on potential damage by commercial aircraft, has put in place imminent threat procedures that will allow reactor operators to place their plants in the safest possible configuration prior to impact, the configuration from which recovery operations using extensive damage mitigation guidelines (EDMGs) currently under development have the greatest opportunity to prevent any public health effects.

As NRC has said repeatedly, our research showed that in most (the vast majority of) cases an aircraft attack would not result in anything more than a very expensive industrial accident in which no radiation release would occur. In those few cases where a radiation release might occur, there would be no challenge to the emergency planning basis currently in effect to deal with <u>all</u> beyond-design-basis events, whether generated by mother nature, or equipment failure, or terrorists. This is because of the plant's inherent capabilities augmented by the imminent threat procedures and EDMGs mentioned above.

Given the measures the Commission has put in place over the past five years, "beamhenges" would provide almost no additional protection at exorbitant cost. In my view a requirement to install "beamhenges" at power reactors would far exceed the NRC's statutory mandate to provide <u>reasonable</u> assurance of <u>adequate</u> protection of public health and safety. Such a requirement would be an excursion into an <u>absolute</u> assurance of <u>perfect</u> protection mandate. While the four petitioning groups may support such a mandate, they will need to change the law first. And while petitioning Congress for such a statutory change, they might explain why that standard should only apply to nuclear regulation, not automobile regulation, or food regulation, or pharmaceutical regulation, or chemical sector regulation.

The second point raised in the December 11, 2006 letter from the four groups claims the staff proposal provides inadequate protection against ground assaults by terrorists. The design basis threat is the threat against which (under 10 CFR 73.55) licensees must be able to defend with high assurance. To meet that threat nuclear power reactor licensees employ about 8,000 security officers at 64 sites, an average 125 per site, 25 per shift (assuming 5 shifts - 4 to cover the 168 hours in a week, and the 5th to account for leave, training, etc.). These well-armed, well-trained officers would defend against an attack from protected positions behind multiple layers of deterrent fencing and barriers. Thus, there is substantial capability against beyond-design-basis numbers of aggressors. For an attacking force to have substantial assurance of success against power reactor defense the attackers would likely need a multiple of the defending force's manpower.

The purpose of the design basis threat is to ensure that very substantial capability is present at all 64 sites. We cannot base the DBT on worst-case speculation about potential threats. The 9/11 attacking force was composed of pilots and thugs armed with box cutters. There is no evidence that they had any paramilitary capability or training. But even assuming, for the sake of argument, that a terrorist group could put together a competent force of that size to attack a hardened facility within the United States, the need to train together for the mission would sharply increase their likelihood of detection by law enforcement agencies aided by an alert citizenry. And, as I said above, my judgment is that even if undetected prior to the assault, the terrorists would fail in their mission because of the substantial beyond-design-basis threat capability built into the defenses at power reactor sites.

To repeat, the DBT is the threat defenses are designed against to achieve high assurance. It in no way reflects the limits on the 64 power reactor sites' ability to cope with terrorist threats. The claim made by the four groups that the staff's proposal leaves the plants "unprotected" against large groups is simply wrong. The fact is that power reactors constitute the tip of the spear in our nation's critical infrastructure. Impaling themselves on that spear by attacking one of these sites would be an exercise in futility for the terrorists, and would result in a lot of dead terrorists.

/RA/	January 22, 2007
Edward McGaffigan, Jr.	(Date)

Replacement vote sheet.

for

EDWARD McGAFFIGAN, JR

PER TELECON 1/25/07

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER MERRIFIELD

SUBJECT: **SECY-06-0219 - FINAL RULEMAKING TO REVISE 10 CFR 73.1, DESIGN BASIS THREAT (DBT) REQUIREMENTS**

Approved ✓ Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below___ Attached ✓ None ___

SIGNATURE

12/4/06
DATE

Entered on "STARS" Yes ✓ No ___

Commissioner Merrifield's Comments on SECY-06-0219
"Final Rulemaking to Revise 10 CFR 73.1, Design Basis Threat (DBT) Requirements"

I approve the publication of the final rule for 10 CFR 73.1 as well as the closure of the Petition for Rulemaking (PRM)-73-12 subject to the attached edits.

The staff should be commended for providing a well organized final rule package. The staff has presented a cogent discussion that describes how the twelve factors set forth in Section 651 (a) of the Energy Policy Act were considered during this rule making and describes the changes made to the final rule as a result of the staff's consideration of the twelve factors, as well as other public comments including the Petition for Rulemaking from the Committee to Close the Gap. The staff should also be commended for developing the rule information in a manner that permits the public to actively participate in the process without compromising safeguards and classified information.

12/4/06

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 who operate as one or more teams, attacking from one or more 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 ~~includes~~ 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. 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~~ several comments specifically fell under this factor. One commenter stated that the NRC needs to engage independent experts to develop a comprehensive computer vulnerability and cyber attack threat assessment, 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 XXX (3150-AG-63)], 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 they are indeed substantial. Furthermore, the land vehicle bomb assault may be coordinated with an external assault, maximizing its destructive potential.

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, and 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;

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 ~~because~~ 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 Nations 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

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 ~~threats that it considers to be~~ 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, onsite security would continue to respond with a graded reduction in effectiveness. The Commission is confident that a licensee's

access to the classified and safeguards-information 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. Unfortunately, language in a *Federal Register* document granting NEI's request for a 30-day extension of the comment period could be read to suggest otherwise. *See*, 71 FR 3791; January 24, 2006. The NRC shared the draft ACDs and RGs with NEI and licensees because licensees (unlike other stakeholders) need that guidance in order to develop licensee protective strategies, as is stated in the *Federal Register* document. The NRC also shared these documents to get specific comments on the RGs and the ACDs that the NRC is producing in parallel with the rule. The ACDs or RGs were not needed to comment on the rule itself. The NRC's decision to extend the public comment period at the same time that it made classified and SGI guidance documents available admittedly caused some confusion on this point. However, 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

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 and found that there would be no significant environmental impact associated with implementation of the proposed rule if adopted; and therefore, concluded that no EIS was necessary. *See*, 70 FR 67387; November 7, 2005. NEPA only requires that the Commission consider the "reasonably foreseeable" environmental effects of its actions in determining whether an EIS is necessary. *See*, 40 CFR.1508.8(b). Effects that are remote, speculative, or embody the worst-case outcome of a particular action do not require an EIS.[1] 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 would be ~~incredibly~~ speculative~~, if not impossible~~. NEPA does not require such an endless inquiry.

The Commission does not agree that the NEPA process would provide a better forum for disclosure and discussion of the DBT rule than this rulemaking action. It is not clear how publishing an EIS for public comment would result in the disclosure of additional information

---

[1]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 the 9th Circuit's a recent decision in the 9th Circuit Court of Appeals. See *San Luis Obispo Mothers for Peace v. NRC*, 449 F.3d 1016 (9th Cir. 2006). However, ~~a~~ determination that the potential environmental effects of a terrorist attack as a result of the licensing of an Independent Spent Fuel Storage Installation should be considered, does not necessarily lead to the conclusion that such effects should ~~also~~ be considered as part of this rulemaking action

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 ~~the mere desire~~ 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 safeguards information 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

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

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, ~~the commenter should be informed that~~ 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 ~~as an effort to mitigate this concern~~ related to this issue. For instance, the Commission has proposed a rule that would amend its regulations related to security requirements for power reactors, [Proposed Rule, Power Reactor Security Requirements, 71 FR XXX (3150-AG-63).] Also, the Commission is proposing to add new requirements to its regulations requiring applicants to assess specific design features that would be incorporated into the final design to support overall security effectiveness of nuclear power plants, [Proposed Rule, New Power Reactors/Security Assessment, 71 FR XXX (XXX-XX-XX).]

With respect to the 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, ~~individually, a large majority of~~ existing fire protection exemptions ~~had~~ have a small ~~or very 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.

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, [Power Reactor Security Requirements, 71 FR XXX (3150-AG-63)], 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.

(~~A~~) Previous Rule: (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 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: (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), 73.1(a)(2)(iv). Licensees subject to the provisions of § 72.212 are exempt from § 73.1(a)(1)(iv).

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

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

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: **COMMISSIONER JACZKO**

SUBJECT: **SECY-06-0219 - FINAL RULEMAKING TO REVISE 10 CFR 73.1, DESIGN BASIS THREAT (DBT) REQUIREMENTS**

Approved X w/edits ___ Disapproved X w/edits Abstain _____

Not Participating _____

COMMENTS: Below___ Attached X ___ None ___

SIGNATURE

12/13/06

DATE

Entered on "STARS" Yes X No ___

Commissioner Jaczko's Comments on SECY-06-0219
Final Rulemaking to Revise 10 CFR 73.1, Design Basis Threat Requirements

I approve in part and disapprove in part the draft final rule amending 10 CFR 73.1 to strengthen the security requirements for licensees subject to the following changes and comments. Additionally, I have several substantive edits to the Statement of Consideration.

I approve in general of the DBT as a broad framework for establishing what licensees have to meet to ensure high assurance. There is much discussion about specific characteristics of the adversary that makes up the DBT. The details of that adversary are described in Commission guidance documents such as the Advisory Characteristics Document (ACD). As long as a capability of the adversary is within the scope of the broad DBT and is shown by intelligence analyses to be an appropriate adversary characteristic it should be included in this guidance document. I believe, with several specific exceptions described below, the DBT provides the appropriate broad framework to give the Commission flexibility to offer modifications, as necessary, based upon intelligence analyses.

I do believe, however, there is a limitation on the capabilities the Commission can expect a licensee to deploy to protect against the DBT. There are some conceivable adversary characteristics that could only be defended against using capabilities reserved exclusively to the military. If it became necessary to add those capabilities to the adversary characteristics document, clearly that would cross the line drawn in 10 CFR 50.13 which states that licensees are not required to defend against attacks "by an enemy of the United States...[or] use or deployment of weapons incident to U.S. defense activities." Thus, the limit on what can be asked of a private guard force is not related to financial constraints. Instead it should be related to the point at which the federal government would be required to promote the formation of private para-military forces to protect critical infrastructure. The resources and capabilities necessary to defend against such a capability falls within the definition of enemy of the state and should be a federal government responsibility. I believe the Commission should add clarity to that definition and intend to more fully address this issue below.

Specifically, there are two areas of the DBT that do not provide the necessary flexibility to allow the Commission to make adjustments based upon intelligence information about adversaries, and I, therefore, disapprove these aspects of the rule. I am not, however, intending to suggest that there is information that is not being appropriately considered, only that the process to do so should be improved.

First, the draft final DBT currently includes a requirement to defend against a land and/or waterborne vehicle bomb assault in 10 CFR 73.1(a)(1)(E) and 73.1(a)(2)(E). Press reports have indicated the use of multiple vehicle bombs overseas. For clarification purposes, these sections of the DBT should be modified to make it clear that this provision includes the potential use of multiple vehicles containing bombs.

Second, the DBT should allow for the possibility of air-based assaults - meaning the deployment of a DBT attack force through the air - just as the DBT currently envisions land-based or water-based forces. I believe this would provide the necessary flexibility should the intelligence information ever indicate that this is a viable method for deploying an adversary force.

I also have some concerns regarding the impression that there should be a difference between the adversary characteristics for the radiological and theft DBT. As the staff indicates, the legal requirement - the high assurance of protection against the DBT - is the same for both DBTs. In general, the composition and capabilities of the adversary forces should also be the same for both. I believe any differences should instead be the result of the different strategic objectives of the adversary in each case.

Apart from the rule there are several issues that I believe the Commission should clarify in order to improve the implementation and effectiveness of the DBT rulemaking.

First, the Commission has no publicly available criteria that establish how the Commission determines what characteristics are included in the adversary characteristics description. I believe the Commission and stakeholders would benefit from a public Commission policy on how this decision is made.

Second, the Commission has not adequately defined "enemy of the state." Therefore, the Commission should clarify this section of our regulations in a separate rulemaking to establish where the enemy of the state line is and then work with our federal partners and Congress to establish comprehensive and executable integrated response plans for the federal protection of these facilities from any threats which exceed that limit. Several comments received on this rule also raise concerns in this area, including NEI, whose comments raised the importance of defining the appropriate boundary between the public and private sectors, and the Mothers for Peace who read an implied cost consideration into the lack of discussion otherwise. Given the importance of this issue and the continuing obvious ambiguity surrounding its meaning, I believe we should address this much-needed clarification.

As an additional step, I propose that staff work with the U.S. Department of Homeland Security to explore establishing an integrated response force modeled on the Urban Search and Rescue (USAR) program that assists victims of structural collapses in major disasters. The USAR program provides training and equipment to local firefighters, doctors, and emergency medical technicians to form teams of experts that are deployed as federal government assets. A comparable program of federal, state, and local low enforcement teams who train together at NRC-regulated facilities and could be deployed to defend and/or take them back from a better-defined beyond DBT "enemy of the state" would provide a higher degree of reasonable assurance of adequate protection.

Finally, I do not disapprove of excluding the aircraft threat from the DBT because the agency has required mitigative strategies to limit the negative consequences of the effects of large fires and explosions for the current fleet of reactors. I strongly believe, however, that any new nuclear power plants built in this country should be designed to withstand commercial aircraft crashes and I intend to propose that the NRC establish such a regulatory requirement in my vote on the Commission paper detailing security requirements for new plant designs (SECY-06-0204).

12/13/06

Gregory B. Jaczko Date

adversary entry points.

Public Comment: Several commenters specifically challenged the proposed rule's consideration of the events of September 11, 2001, expressing concern that the DBT rule does not require licensees to defend against a number of attackers comparable to the 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. ~~they are indeed robust.~~ The DBTs are the result of the NRC's continuous evaluation of current threats. That evaluation is not limited to a particular kind of

characterized as addressing Factor 2, only several comments specifically fell under this factor. One commenter stated that the NRC needs to engage independent experts to develop a comprehensive computer vulnerability and cyber attack threat assessment, 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 XXX (3150-AG-63)], 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 ~~but they are indeed substantial.~~ Furthermore, the land vehicle bomb assault may be coordinated with an external assault, maximizing its destructive potential.

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.

The answer to these comments should be more clearly explained.

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 address protective strategies and security measures for nuclear power plants and other licensed facilities under waterborne attacks, and require licensees to defend against the DBTs. [Proposed Rule, Power Reactor Security Requirements, 71 FR XXXX (3150-AG-63).] In Summary:

- NRC Position: Agrees with the 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.

Explain how this increases flexibility

Public Comment: Refer to Factor 2.

Should allow for multiple vehicles.

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.)

the NRC is continuing to perform studies & evaluate

Should make it clear that the effects on these facilities

The NRC is continuing to perform studies to evaluate the effects of spent fuel fires.

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 offsite emergency plans such that the NRC's emergency planning basis remains valid (*See*, Key Radiological Protection Mitigation Strategies Order, 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

AFFIRMATION ITEM

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER LYONS

SUBJECT: **SECY-06-0219 - FINAL RULEMAKING TO REVISE 10 CFR 73.1, DESIGN BASIS THREAT (DBT) REQUIREMENTS**

Approved X w/edits Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below___ Attached X None ___

Peter B. Lyons
SIGNATURE

11/ 28 /06
DATE

Entered on "STARS" Yes ✓ No ___

Commissioner Lyons' Comments on SECY-06-0219

I approve the final rule amending the 10 CFR 73.1 Design Basis Threat (DBT) requirements.

I have carefully considered the Congressional mandate in Section 651 of the Energy Policy Act (EPAct), public comments on the draft proposed rule, and the staff's analysis of both. I believe the staff has very appropriately met the EPAct mandate with a sound and well articulated analysis. Also, I believe the degree of detail presented in the proposed rule language afforded an adequate and appropriate opportunity for public input, and I appreciate and value the degree of public interest and input this proposed rule change has engendered. Public comments expressing the view that the DBT should include air-based threats were a prominent aspect of this interest. I support the staff's analysis, both in regard to the EPAct and in addressing the public comments on this issue. Also, I would like to add some additional thoughts as follows.

First, I believe that NRC is playing its proper role as a partner in intelligence gathering and information sharing, and by maintaining an intelligence assessment capability to provide timely new threat information to the Commission that may warrant NRC regulatory action. The nature of the threats that face our Nation today have evolved since September 11, 2001, and will continue to do so into the future, including possible threats that could target our critical infrastructure with weapons and delivery methods not previously used. Our Nation has appropriately responded to these evolving threats by pooling and integrating our federal, state, and local governmental resources to enable the necessary degree of constant vigilance and readiness to respond.

This evolving nature of nation-wide threats make it ill-advised in general for our regulations to become overly focused on a specific threat, particularly those being adequately addressed by integrated national efforts. Such approaches can potentially waste resources and direct attention away from possible new threat scenarios for which we must be flexible in adjusting our defenses if necessary, both at the national level and through new regulatory requirements imposed on our licensees if needed. Although the public discourse on the issue of air-based threats has been constructive and informative, the NRC must be disciplined and objective in determining where to best allocate the time, attention, and resources of both our staff and licensees. I believe the current plant mitigation strategies in place today provide the level of protection appropriate for the current air-based threat given the national response to air safety and the relatively robust nature of licensee facilities. We must continue to maintain our vigilance on the entire landscape of possible threats.

In summary, I am convinced that, through the dedicated efforts of many agencies, air-based threats have been substantially reduced, that NRC regulations are appropriately focused based on current threat assessments, and that NRC remains appropriately responsive to emerging threat information.

Peter B. Lyons 11/28/06

Peter B. Lyons Date

and not adequately mitigated by other measures.

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 bases the DBT adversary tactics on those 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

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, and 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;

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 and found that there would be no significant environmental impact associated with implementation of the proposed rule if adopted; and therefore, concluded that no EIS was necessary. *See*, 70 FR 67387; November 7, 2005. NEPA only requires that the Commission consider the "reasonably foreseeable" environmental effects of its actions in determining whether an EIS is necessary. *See*, 40 CFR.1508.8(b). Effects that are remote, speculative, or embody the worst-case outcome of a particular action do not require an EIS.[1] 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 would be ~~incredibly~~ speculative, at best. ~~if not impossible.~~ NEPA does not require such an ~~endless~~ inquiry.

The Commission does not agree that the NEPA process would provide a better forum for disclosure and discussion of the DBT rule than this rulemaking action. It is not clear how publishing an EIS for public comment would result in the disclosure of additional information

---

[1]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. See *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 also be considered as part of this rulemaking action.

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 ~~the more desire~~ 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 safeguards information 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

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, ~~the commenter should be informed that~~ 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. ~~as an effort to mitigate this concern~~. For instance, the Commission has proposed a rule that would amend its regulations related to security requirements for power reactors, [Proposed Rule, Power Reactor Security Requirements, 71 FR XXX (3150-AG-63).] Also, the Commission is proposing to add new requirements to its regulations requiring applicants to assess specific design features that would be incorporated into the final design to support overall security effectiveness of nuclear power plants, [Proposed Rule, New Power Reactors/Security Assessment, 71 FR XXX (XXX-XX-XX).]

With respect to the 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 ~~individually, a large majority of~~ existing fire protection exemptions have had a small ~~or very 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.