Entergy

PR 50, 72 and 73
(71FR62663)

Entergy Nuclear
P.O. Box 31995
Jackson, Mississippi 39286-1995
Tel 601-368-5758

F. G. Burford
Acting Director
Nuclear Safety and Licensing

38

CNRO-2007-00017

March 23, 2007

Ms. Annette L. Vietti-Cook
Office of the Secretary
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Rulemaking and Adjudication Staff

Subject: Request for Comments on Proposed Power Reactor Security Requirements, 71Fed. Reg. 62664 – 62874 dated October 26, 2006 (RIN 3150-AG63)

Dear Ms. Vietti-Cook:

Entergy Nuclear (Entergy) is pleased to submit our comments in the above captioned matter. Entergy is a long standing member of the NEI Security Working Group and the NEI Task Force that reviewed the subject rulemaking. Entergy participated in the development of industry comments on the proposed security rule. Those detailed comments are not duplicated here. We specifically endorse the comments and examples submitted by the Nuclear Energy Institute (NEI) by their letter dated March 26, 2007 and Entergy offers our additional perspectives and comments herein.

Overarching Comments
Significant industry security resources and significant NRC staff review resources have been invested since 9-11-2001 in a top to bottom review and strengthening of the security posture of U.S. nuclear facilities which represented then and continues to represent now the pinnacle of industrial security worldwide. Approximately 50 force-on-force (FOF) exercises completed after 9-11-2001 have repeatedly demonstrated superior industry security force ability to defend against the newest design basis threats of radiological sabotage.

The primary goal of the rulemaking was to codify the post 9-11 orders into security regulations. Entergy had institutionalized the order requirements through NRC approved industry guidance (NEI 06-12) and NRC approved revisions to site security plans. Properly constructed, the proposed rules should have minimal impact on the existing security plans. We believed this to be the Commission's intent. We agree the patchwork of regulatory fabric which comprises the regulatory requirements through new statutes, regulations, orders and guidance needs to be consolidated via rulemaking that incorporates orders and statutes into rules. Specifically, the Energy Policy Act of 2005 requirements should be and have been included and the order requirements that industry has implemented should be codified as imposed. Any other new requirements should not be concealed in staff "clarifications" but should be examined based on their own merit and demonstrated need.

Template = SECY-067

SECY-02

New requirements not in current orders will impact existing plans, existing procedures, existing training, and existing industry guidance documents and divert security and supporting plant resources for administrative changes. This would require significant licensee rewriting and another NRC approval and implementation cycle. The diversion of security attention from the defense of the operating facility to additional revisions to recently NRC approved Security Plans is counter productive and inimical to the common defense and security at a time when security focus and stability is paramount in the current threat environment.

Incorporating NRC Orders which contain safeguards information into public rulemaking certainly presents unique challenges. The approach taken to develop broad security rule language to protect details which might give a potential adversary undue knowledge of defensives and use safeguards guidance documents for these details reverses the traditional approach and establishes potentially untested regulatory precedents. Typically the rules define the limits and the guidance establishes acceptable methods for meeting the requirements. Entergy's full understanding of the potential impacts of the proposed rule changes have been impacted by the unavailability of the implementing guidance documents.

As was evidenced during the recent public meeting, rule language being proposed is often ambiguous in that it does not always implement staff intent; what it says can be read to require more than what may have been intended. This language must be revised until it contains a single regulatory meaning only. To not do so would introduce considerable confusion and instability into the inspection process and tie up licensee and regional resources in avoidable controversy about what was intended (vice how it can be read). To prematurely publish a rulemaking flawed in such a way would be contrary to the Commission's principles of good regulation. While it is evident that considerable staff work (many man years) went into drafting the hundreds of pages of rulemaking, it is equally evident that more work is required.

Regulatory Analysis
The Regulatory Analysis does not address all changes, many of which can represent significant new investments that have not been justified or it underestimates the impacts. The rulemaking was developed on an accelerated rulemaking schedule that limited stakeholder participation[1]. The regulatory analysis is predicated on a significant increase in public safety. To the extent that it accurately codifies orders predicated on public health and safety, we have no comment. The industry is already in full compliance with the requirements of the orders. Where the proposed rule does not accurately reflect the original orders, we are not in agreement. Additionally, rule language has been moderately to extensively changed in most other areas that inherently claim the same significant increase in public safety and are not individually justified as required by the administrative procedures requirements.

The change of a single word (e.g., back up power to uninterruptible power) can have a huge cost and implementation schedule impact. In the absence of the implementing guidance documents we can read the new language to impose numerous changes with implementation

[1] Draft Regulatory Analysis at page 11

costs that could sum into the billions of dollars industry wide. The implementation schedules cannot be accurately predicted but would be measured in years.

The regulatory analysis quantitatively evaluates 20 identified changes. Without stakeholder input the cost to industry was determined to be $288 - $394 million Net Present Value. We believe these estimates are significantly low. For example, uninterruptible power was estimated at $46,200. One Task Force licensee expended over $100,000 for uninterruptible power to security lighting alone. Without the benefit of the implementing guidance documents we estimate the changed language can be read to require at least $20 million per site to as high as $60 million per site for the identified and unidentified changes.

73.55

The existing performance objective of preventing radiological sabotage has been transmuted into "designed to prevent significant core damage and spent fuel sabotage through the coordinated implementation of specific actions and strategies required to intercept, challenge, delay, and neutralize threats up to and including the design basis threat of radiological sabotage" throughout the proposed regulations. Simply stated the roles of access authorization and physical security are to 'let the good guys in' and 'keep the bad guys out'. The performance standard for security is correctly to defend against radiological sabotage; to defend target set elements with a view toward preventing core damage (and similar damage to spent fuel in the pool), which could directly or indirectly endanger public health and safety by exposure to radiation. Stated another way, if all elements of a target set are compromised it is logically assumed that core damage could be the result. The staff has logically reversed the performance standard to be that security's goal is to prevent core damage and spent fuel pool sabotage including plant actions for mitigation of these end states. This is a logical fallacy because the conclusion does not follow from the premises. If security responsibility for stopping adversaries prevents core damage, then making security responsible for preventing core is a logical fallacy[2]. The rule should consistently maintain the objective stated in 73.1 of protecting against radiological sabotage[3]. Entergy endorses NEI comments and examples of inadequate rule language wording.

Appendix C

Entergy endorses detailed NEI comments. That the Interim Compensatory Measure (ICM) and other order requirements need to codified and that the original order requirements were contained in a documents broadly referred to as "security orders" does not mandate that all such requirements belong in security regulations. [e.g., 73.55] Indeed many of the

---

[2] If A then B therefore if B then A is logically false. Any argument that takes the following form is a non sequitur: If A is true, then B is true. B is stated to be true. Therefore, A must be true. Even if the premises and conclusion are all true, the conclusion is not a necessary consequence of the premises. This sort of non sequitur is also called affirming the consequent.

[3] This concept is contrary to the security objective as defined in 73.55 which states "...a security organization which will have as its objective to provide high assurance that activities that involve special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to public health and safety. The physical protection program must be designed to detect, assess, intercept, challenge, delay and neutralize threats up to and including the design basis threat of radiological sabotage as stated in 73.1 at all times."

enhancements had nothing whatsoever to do with physical security; they dealt with advanced fire fighting strategies, new operations mitigation strategies, and emergency planning recovery strategies. Many of the scenarios are well beyond both the design basis threat (DBT) for radiological sabotage and the design basis and licensing basis of the plant. Proposed changes to the contingency plan force detailed procedures unrelated to security into the contingency plan and specifically prohibit reference to other plant procedures. This will adversely impact how operations, Emergency Planning (EP) and other organizations perform their recovery functions; require significant procedural changes and corresponding retraining for no stated valid reason.

The details in Appendix C go well beyond the overarching requirements in 73.55 pertaining to security duties, especially with respect preventing core damage and are fundamentally flawed. We believe tying prevention of core damage as a security performance responsibility and measure confuses the true security objective of defending target set elements, the loss of which may result in core damage. This construction is an illogical extension of security responsibility and creates numerous interface issues with operations, emergency planning and other plant procedures and processes.

Appendix C, as proposed too broadly attempts to make the safeguards contingency plan encompass the entire integrated plant response to all postulated events including those beyond the DBT (i.e, large fires also known as ICM B.5.b). The integrated response plan has been expanded to integrate operations, emergency planning and other unrelated procedures. Specific Statement of Considerations (SOC) language in the appendix forbids reference to other site procedures. The phrase "To the extent that the topics are treated in adequate detail in the licensee's approved physical security plan, they may be incorporated by cross reference to that plan" would be deleted because this information would be required to be specifically detailed in contingency planning" [Section 3(e)]

B.5.b is a broad strategy to employ readily available resources to mitigate the consequences of a large area fire or explosion. There is no security force component to effectively intercept, challenge, delay or neutralize any non ground assault related threat. The plant response involves, plant operations actions, fire fighting and offsite emergency response coordination which have no place in the safeguards contingency plans. Safeguards contingency plans have historically dealt with security organization defensive responses. This same structure continued to be used in revised contingency plans implementing the orders approved by the Commission as recently as late 2004. Short of admitting responding offsite resources, security has no defined recovery role. These mitigation topics are properly the subject matter of the operations and emergency response procedures not the security procedures. Security goals are designed to interdict attempts to disable target set elements. Failure (of the adversaries) to compromise all elements of a target set is assumed to not result in core damage or spent fuel sabotage. However, the approach being attempted in the revised contingency plan is to regulate licensee mitigation plans for plant damage including extreme plant damage which is not a security function or part of the DBT for radiological sabotage.

The Commission is already deploying a different and more appropriate regulatory scheme for addressing B.5.b conditions. B.5.b is being controlled with a performance based license

condition that is satisfied by voluntary licensee commitments to B.5.b Phase 2 and Phase 3 voluntary strategies. This regulatory scheme completely negates the need for any of the proposed changes or clarifications to Appendix C to cover "How the onsite response effort is integrated to include specific procedures, guidance, and strategies to maintain or restore core cooling, containment, and spent fuel pool cooling capabilities using existing or readily available resources (equipment and personnel) that can be effectively implemented under the circumstances associated with loss of large areas of the plant due to explosions or fires." Putting this specific detail in the contingency plan actually limits the effectiveness of licensee strategies for dealing with unpredictable plant end states. The existing regulatory approach and language should be retained (i.e., retain the current security focused content of the safeguards contingency plans). For future new plant licensing, regulations regarding B.5.b would be more appropriately located in Subpart C of 10 CFR 52. It is recommended that the B.5.b regulation, proposed for 10 CFR 52, simply consist of the performance based language that is being used for the license conditions being issued to existing licensees. This regulation would be applicable to new licenses issued after the effective date of the regulation thus existing licensees would retain their B.5.b license condition for the remainder of their license.

Appendix C paragraph J.2.ii for example now requires that B.5.b mitigating strategies be relocated to an integrated response plan under security. These strategies are generally operations procedures that operate in conjunction with Emergency Operating Procedures, Severe Accident Mitigation Guidelines and Extreme Damage Mitigation Guidelines for beyond design base conditions. This is an inappropriate expansion of the security role or the roles of security programs in the hierarchy of plant procedures and processes. The expanded Contingency Plan likewise usurps longstanding emergency plans which are beyond the purview of the DBT.

The Performance Enhancement Program is not a contingency response. These are training requirements that should be relocated from the contingency plan.

Cyber Security
Entergy endorses detailed NEI comments. We find good agreement between NEI-04-04 and the proposed rule. However, cyber security and its mitigation is not a physical security issue and should be relocated from the contingency plan. Some of the detail is more appropriate for guidance documents.

Appendix B Training
Entergy endorses detailed NEI comments. Appendix B Training has incorporated much of the detailed guidance of NEI 03-09 as regulatory requirements. This detail is more appropriate as guidance vice requirement. The inclusion undermines standardization by reintroducing site specific detail that is better contained in implementing procedures alone.

73.56 Access Authorization
Entergy endorses detailed NEI comments. Entergy is concerned that the proposed language requires psychological reassessment of individuals within five years of the date on which it was last completed. This is a new requirement with significant cost and negligible benefit. Since all other aspects of the access authorization requirements are repeated at the five year

interval already, and the Behavior Observation Program is continuous, nothing is gained by repeating the psychological reassessment. While the industry sees the need for the psychological assessment for granting access authorization, the continuous Behavior Observation Program obviates the need for such a reassessment for an individual maintaining access.

73.18/73.19 Enhanced Weapons
Entergy endorses detailed NEI comments. Entergy has no additional comments on codifying the Energy Policy Act of 2005.

Appendix G Reporting
Entergy endorses detailed NEI comments. Entergy believes unnecessary reporting may be increased.

73.58 Safety Security Interface
Entergy endorses detailed NEI comments. Use of the term "all procedures" creates a population of plant procedures that would be unmanageable for security to be cognizant of. This proposed rule needs to be revised to take credit for existing management programs that are in place and only impose changes related to the security plan and implementing procedures in a security regulation.

Conclusions
It is of paramount importance that the final security rulemaking be carefully crafted and not rushed through judgment to meet an unnecessary timeline. Each licensee currently has a recently NRC approved Security Plan that incorporates all Post 9-11 orders and new requirements; Licensees have demonstrated through up to date NRC FOF tactical exercises the ability to effectively defend against the most current Design Basis Threats of radiological sabotage. Entergy encourages the commission to permit the industry to work with the staff following the close of the public comment period to resolve industry (and Entergy) comments and corresponding safeguards regulatory guidance to achieve clarity and single purpose.

Sincerely,

FGB/LAE/bal
cc:
Mr. D. J. Walters (NEI)

From: Carol Gallagher
To: SECY
Date: Tue, Mar 27, 2007 2:48 PM
Subject: Comment letter on Power Reactor Security Requirements

Attached for docketing is a comment letter on the above noted proposed rule from F. G. Burford, Entergy Nuclear, that I received via the rulemaking website on 3/26/07.

Carol

Mail Envelope Properties (46096701.A59 : 5 : 35764)

Subject:	Comment letter on Power Reactor Security Requirements
Creation Date	Tue, Mar 27, 2007 2:48 PM
From:	Carol Gallagher
Created By:	CAG@nrc.gov

Recipients
nrc.gov
TWGWPO02.HQGWDO01
SECY (SECY)

Post Office	**Route**
TWGWPO02.HQGWDO01	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	583	Tuesday, March 27, 2007 2:48 PM
TEXT.htm	452	
1785-0032.pdf	142382	Tuesday, March 27, 2007 2:46 PM

Options

Expiration Date:	None
Priority:	Standard
ReplyRequested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard

Junk Mail Handling Evaluation Results
Message is not eligible for Junk Mail handling
Message is from an internal sender

Junk Mail settings when this message was delivered
Junk Mail handling disabled by User
Junk Mail handling disabled by Administrator
Junk List is not enabled
Junk Mail using personal address books is not enabled
Block List is not enabled