DOCKET NUMBER PR 73
PROPOSED RULE
(65FR 36649)

Entergy

Entergy Operations, Inc.
1340 Echelon Parkway
Jackson, Mississippi 39213-8298
Tel 601-368-5758

Michael A. Krupa
Director
Nuclear Safety & Licensing

'00 OCT -6 P2:51

CORRECTED COPY TO CORRECT INCORRECT CNRO NUMBER

August 23, 2000

Ms. Annette 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 Re-evaluation of Physical Protection Regulations, 65 Fed. Reg. 36649 (June 9, 2000)

Reference: *Federal Register* Vol. 65, No. 112, Pages 36649 – 36651, dated June 9, 2000

CNRO-2000-00029

Dear Ms. Vietti-Cook:

Entergy Operations, Inc. (Entergy) is pleased to submit our comments in the above captioned matter. Entergy is a member of the NEI Security Working Group and also participated in the development of NEI's comments. We endorse the comments submitted by the Nuclear Energy Institute and Entergy offers our additional perspectives and comments herein. We believe our nuclear facilities are among the most secure facilities today presenting a hard target to potential adversaries and that NRC's OSRE program yielded beneficial insights. Voluntary enhancements by industry have strengthened our security posture. However, we also believe that regulatory processes (including security) need to be stable and predictable and that new requirements must pass the prescribed backfit tests prior to implementation. Prescriptive regulations do not necessarily assure that regulatory objectives are met

On June 9, 2000, the NRC published in the *Federal* Register a request for comments on the staff proposal outlined in SECY-00-63. The Staff requirements Memorandum (SRM) related to SECY-99-241 asked the staff to address (a) the attributes of the design basis threat and b) the definition of radiological sabotage. SECY 0063 responds to (b). We find that the staff's proposals are not responsive. Instead of a definition of radiological

Template = SECY-067 SECY-02

sabotage, (which already exists) the staff proposes new prescriptive sabotage induced event sequences the licensees are expected to defend against. These proposed new standards are not justified. SECY-00-63 argues against the use of prescriptive requirements in part because the way licensees will understand them and in part due to how the NRC will inspect and enforce them. Entergy does not understand this new concept of critical safety function and believes their use will perpetuate the same problems of implementation while clouding what 'unreasonable risk' to the public health and safety actually is. Lack of clarity in what is safe or not safe will not enhance public confidence. For the reasons outlined here and in the attached paper, Entergy does not support the staff's proposal.

We agree with the staff that there are longstanding issues with the implementation of 10 CFR 73.55 requirements at power reactors. Specifically, that implementation of these requirements through compliance with the prescriptive requirements of the physical protection plans written in accordance with 10 CFR 73.55(b) through (h) are problematic due in part to the way the requirements were (a) understood by the licensees and (b) inspected and enforced by NRC. However, overall site security and the security organization's readiness to respond to an adversary attack were tested and confirmed during regional inspection activity and OSREs. Entergy supports a comprehensive review of the security regulations and clear definition of the attributes of the design basis threat that can result in the industry implementing a performance based self evaluation of its security program effectiveness.

The security objective as stated in10 CFR 73.55 is that the licensee shall establish and maintain an onsite physical protection system and security organization which will have as its objective 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. The performance standard for security, as it is for all other aspects of nuclear plant design and operation, is protection of public health and safety. There is not a higher standard than protection of public health and safety. The standard as it is stated begs the question of what constitutes an "unreasonable risk".

10 CFR Part 100 establishes that there is a substantial base of knowledge regarding power reactor siting, design, construction and operation and that base reflects the primary factors that determine public health and safety. Siting factors and criteria are important in assuring that radiological doses from normal operation and postulated accidents will be acceptably low, and that natural phenomena and potential man-made hazards will be appropriately accounted for in the design of the plant, that site characteristics are such that adequate security measures to protect the plant can be developed and that physical characteristics unique to the proposed site that could pose a significant impediment to the development of emergency plans are identified. "Successful" radiological sabotage would then need to endanger public health and safety by unreasonable risk to radiological exposure.

For radiological sabotage to be successful, the malevolent activities would have to lead to a large radiological release that exceeds 10 CFR Part 100 limits. The industry's

[1] NUREG 1178 ("Vital Equipment/Area Guidelines Study," page 4-1

understanding of radiological sabotage is supported by that expressed in NUREG 1178:[1]

"*Successful radiological sabotage results in doses in excess of those defined in 10 CFR 100. The 10 CFR 100 criteria are intended to serve as a benchmark for the analysis of major events, that is, those events that pose a potential health hazard (a significant release of radioactivity as a result of a major accident or radiological sabotage*)."

However, Entergy does not suggest that security effectiveness be measured on Part 100 releases. While Part 100 establishes adequate protection of public health and safety, a plant's response to a security threat is more clearly measured in its ability to prevent significant core damage. {"Significant core damage" is used vice "no core damage" to preclude claiming a pin hole leak is "core damage". A numerical value greater than zero could easily be established.}

Clearly, without significant core damage, there can be no threat of radiological release and therefore no radiological dose to threaten or endanger the public health and safety. Without significant core damage there can be no "unreasonable risk". In fact, throughout force-on-force drills conducted pursuant to the Regulatory Effectiveness Review (RER) program and the Operational Safeguards Response Evaluation (OSRE) program the staff and industry have usually used prevention of significant core damage as its measure of success in defending against radiological sabotage. This measure provides margin to a Part 100 release just as Part 100 release limits provide margin in protecting public health and safety. We see no need to further escalate that threshold now.

Thank you for the opportunity to provide these comments. Entergy looks forward to commenting on the attributes of the design basis threat.

Sincerely,

M. A. Krupa

MAK/LAE/baa

cc: Mr. C. G. Anderson (ANO)
Mr. C. M. Dugger (W-3)
Mr. W. A. Eaton (GGNS)
Mr. R. K. Edington (RBS)
Mr. G. J. Taylor (ECH)

Mr. T. W. Alexion, NRR Project Manager, ANO-2
Mr. J. F. Harold, NRR Project Manager, RBS
Mr. N. Kalyanam, NRR Project Manager, Waterford-3
Mr. M. C. Nolan, NRR Project Manager, ANO-1
Mr. S. P. Sekerak, NRR Project Manager, GGNS

[1] NUREG 1178 ("Vital Equipment/Area Guidelines Study," page 4-1

Request for Comments – SECY-00-063
August 23, 2000
CNRO-2000-00029

bcc: Mr. W. B. Abraham (G-SSB1-NSR)
Mr. S. A. Bennett (N-GSB)
Mr. C. A. Bottemiller (G-ADM2-LIC)
Mr. M. K. Brandon (W-GSB-318)
Ms. K. A. Courtney (R-GSB-43)
Mr. L. F. Daughtery (G-SSB1-NSR)
Mr. V. H. Dunn (G-ADM2-PSE)
Mr. R. T. Finch (W-GSB-240)
Mr. D. E. James (N-GSB)
Mr. R. J. King (R-GSB-42)
Mr. J. W. Leavines (R-GSB-43)
Ms. J. M. Manzella (W-GSB-318)
Mr. D. B. Miller (W-GSB-318)
Mr. G. P. Norris (R-GSB-42)
Mr. E. P. Perkins (W-GSB-310)
Ms. S. L. Pyle (N-GSB)
Mr. R. G. Redmond (R-GSB-27)
Mr. J. C. Roberts (G-SSB1-NSR)
Mr. J. D. Vandergrift (N-GSB)
Ms. D. S. Waldron (N-GSB)
Mr. D. R. Williams (N-GSB)
Station Document Control (RBS)
Corporate File [6]

Critical Safety Function Concept Evaluation

In order to cause significant core damage, all redundant means to provide adequate core cooling must be coincidentally defeated. As long as a single capability to provide adequate cooling to the core exists, there can be no postulated core damage. Plant design 'defense in depth' provides numerous redundant and diverse capabilities to cool the core. Additionally, three more barriers exist between the radiological source material in the core and an uncontrolled release; these are the fuel cladding, the reactor coolant pressure boundary and the containment. The siting criteria of Part 100 provides yet another 'barrier', that being time and distance. For security purposes, sets of equipment or "target sets" have been identified for defense strategies. All elements of a target set must be compromised for there to even be a risk of radiological release.

The staff seeks to clarify in SECY-00-63 licensee performance in defending against radiological sabotage by requiring that licensees protect 'critical safety functions' (CSF) as a primary objective of the rule. The assumption is that loss of a critical safety function will necessarily lead to a significant off site release, logically ignoring significant remaining margin and capabilities. (For example, loss of such a single function is immediately assumed to cause the loss of all automatic design features, the loss of all effective operator intervention and use of emergency operating procedures, the loss all cooling capability, the loss of the fuel cladding, the loss of the reactor coolant pressure boundary, the loss of the containment, and renders ineffective all actions of the emergency response organization resulting (with favorable wind conditions) in exposure to the public of doses in excess of 10CFR Part 100 limits.) This concept completely ignores plant design and defense in depth. We believe it sets new undefined regulatory standards for "critical".

Therefore, the concept of critical safety function is not clearly understood, is inconsistent with the existing regulatory scheme because it is not used elsewhere and can only succeed in creating more confusion. This lack of clarity of the significance to public health and safety can not increase public confidence in the plant's security response.

CSF is inconsistent with Target Set loss. By definition, all elements of a Target Set must be compromised or lost to initiate core damage needed to pose any unreasonable risk to public safety. Without core damage there is no radiological threat to the public and no unreasonable risk. The loss of a critical safety function alone is assumed to but may not necessarily result in core damage resulting in an ambiguous standard for both protection and inspection.

The degree to which the of loss of a critical safety function can affect safety ultimately is measured in its resulting in core damage; therefore the existence of core damage is a more clear standard for evaluation of success of a plant's response to a security attack.

Loss of a CSF target (a singular function in a target set) would be construed as a serious violation of the regulations while a public threat has not clearly been established. This would serve to unnecessarily alarm the public about plant safety. A loss of a piece of equipment simulated in a security exercise could be viewed as significantly more risky than a random failure of the same piece of equipment.

Inclusion of CSF in the regulations only serves to create opportunities to cite licensees for limited failures to protect equipment even when that loss may be part of a planned defensive strategy.

The use of CSF will result in continued subjective and therefore inconsistent enforcement of security regulations. Ambiguous security requirements are already recognized by both the staff and industry as an existing problem. Non risk-significant violations unnecessarily erode public confidence and waste NRC and Industry resources, violating two goals of both the industry and NRC in enacting the new Regulatory Oversight Process.

Use of CSF would necessitate reperforming existing target set analysis to the new concept. A backfit analysis must demonstrate that the cost of performing such a required CSF analysis will result in new risk significant target elements being identified that are not already being addressed by current licensee strategies or target sets.

Licensees already use risk significant analysis concepts (similar to protection of critical safety functions) in the identification of their target sets and response strategies. These target sets have been validated by RER and OSREs over the last 8 years. There is no single best way to establish targets sets. Introducing critical target set is a new unnecessary requirement.

CFS may be an alternative way to establish or validate current target sets, that protect public health and safety. Use as regulatory guidance may be more appropriate, not withstanding its lack of clear regulatory meaning.