(1)

NMC

Committed to Nuclear Excellence

'00 JUL 27 P3:51

July 25, 2000

DOCKET NUMBER
PROPOSED RULE PR 73
(65FR36649)

Secretary,
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
Attention: Rulemakings and Adjudications Staff

Re: SECY-00-0063 (Staff Re-Evaluation of Power Reactor Physical Protection Regulations) as published in Federal Register Vol. 65, No. 112 dated June 2000

Dear Sir:

I would like to submit the attached Nuclear Management Company (NMC) comments concerning the issuance of SECY-00-0063. Your efforts to re-evaluate current security regulations is greatly appreciated and it is hoped that changes made will be based upon fact consistent with logic used in other areas of nuclear power regulation.

The SECY discusses three comprehensive and interrelated issues:

1. Revision of 10 CFR 73.55 Requirements.
2. Clarification of "Radiological Sabotage."
3. Industry developed Self-Assessment Program ("Safeguards Performance Assessment").

NMC comments to these issues are addressed in the Attachment. Thank you for considering these comments. Please direct any comments or concerns to David A. Axt of my staff. Mr. Axt can be reached at: 715.377.3341.

Sincerely,

Mark Findlay, Ph.D.
Director of Security
700 First Street
Hudson, WI 54016

Cc: James Davis, NEI

Template = SECY-067

SECY-02

Nuclear Management Company, LLC (NMC)

Comments concerning the issuance of SECY-00-0063 (Staff Re-Evaluation of Power Reactor Physical Protection Regulations) as published in Federal Register Vol. 65, No. 112 dated June 2000

Federal Register Vol. 65, No. 112 requests public comment on three key issues contained in SECY 00-0063:

1. Revision of 10 CFR 73.55 Requirements.
2. Clarification of "Radiological Sabotage."
3. Industry-Developed Self-Assessment Program

NMC comments to these issues are addressed in the following pages.

1. Revision of 10 CFR 73.55 Requirements.

A. *Background*

The current security regulations commenced in the 1970s with little attention on security's protective strategy for defending against an overt attack and attempted radiological sabotage. As such, the industry has experienced a certain degree of "regulation by inspection," resulting in inconsistent and expensive security programs. Physical Security Plan commitments vary widely across the industry and perpetuate unnecessary requirements. Rulemaking that applies risk-informed, performance-based approaches is essential to properly focus program goals and outcomes. The key to any performance-based rule is a clear set of design criteria for which performance can be measured. These criteria should be consistent with other plant design criteria that meet the siting requirements of 10 CFR Part 100. A process is also needed that clearly defines the adversary characteristics used in designing a security program to maintain a hard-target status.

The current security regulations possess several important security elements (physical preventative methods, detection aids, contingency response capabilities, and security managerial systems). The NMC, however, perceives several problems with the current revision process. Specifically, it does not:

- Use *credible threats* as a basis for a risk analysis/management process.
- Give due consideration for the *deterrent* effect of existing security measures.
- Entail *security risk management* techniques.

B. *Credible Threats*

NMC believes that the Staff should consider developing a rational basis for defining the threat, and, therefore, avoid the continual intensification of adversary characteristics. Unfortunately, the Staff is currently contemplating several significant increases to the Adversary Characteristics Description (ACD), many which are beyond that used by the OSRE over the last 10-years.

Adversary capabilities used during OSRE drills have continued to escalate. With each new plant security upgrade, subsequent OSREs develop new defeat methods. This practice has required plants to implement ever increasing physical security measures, such as barriers, razor wire, and hardened defensive bunkers. Additionally, postulated adversary capabilities appear to ignore the fundamental motivation of a terrorist as discussed in NUREG 0459 ("General Adversary Characteristics Summary Report"). Specifically, heavily defended targets, as in the case with all nuclear power plants, are avoided by terrorists. "*One of the least likely methods of attack is an overt armed assault...safeguards planners should avoid preoccupation with this tactic*" (NUREG 0459). The focus needs to be on maintaining plants as a *hard target*, not the capability to counter every hypothetical terrorist capability.

Some of the weapons and capabilities contemplated in the draft Adversary Characteristics Description (ACD) contradict NRC Statements of Consideration (32 FR 13446) where it indicates that commercial nuclear facilities were not expected to protect against such capabilities. Such an escalation may necessitate that site security personnel: (a) receive federal authority to possess like weapons (e.g., automatic weapons), or (b) be protected by US/National Guard military forces.

59FR38889, August 31, 1994 (statement of considerations for 10 CFR 50.13) makes it clear that the scope of that regulation is to relieve applicants of the need to provide protective measures that are the assigned responsibility of the nation's defense establishment. The Atomic Energy Commission recognized that it was not practical for the licensees of civilian nuclear power reactors to provide design features that could protect against the full range of the modern arsenal of weapons.

When incidents involving national security occur, such as those occurring during the Persian Gulf War, nuclear facilities can be placed on "Alert" so that heightened security measures can be put into effect at that time. Nuclear facilities should not be expected to be continuously in a state of "Alert."

C. *Deterrence*

The common characteristics (i.e., the "defense-in-depth" concept of reactor plant design) of commercial power reactors make the release of radioactivity by acts of sabotage difficult. In 50.13 FR, it points out that:

"The massive containment and other procedures and systems for rapid shutdown of the facility included in these features could serve as useful in protection against the effect of enemy attacks and destructive acts, although that is not their specific purpose. One factor underlying the Commission's practices in this connection has been a recognition that reactor design features to protect against the full range of the modern arsenal of weapons are simply not practicable and that the defense and internal security capabilities of this country constitute of necessity, the basic "safeguards" as respects possible hostile acts by an enemy of the United States."

"The circumstances which compel this recognition are not, of course, unique as regards to a nuclear facility; they apply also to other structures which play vital roles within our complex industrial economy."

Therefore, commercial nuclear power plants should not be treated uniquely in this regard, since they are no more of a strategic target or public health hazard than other industries.

In most security contexts, the very existence of significant physical security measures dissuades potential malevolent acts. This has been demonstrated in numerous security studies [1, 2, 3]. According to a report prepared for the US Department of Energy:

"Deterrence is the largely unidentified and untapped component of physical security that might significantly improve security. Despite the difficulty in measuring the success of deterrence, it appears to offer a low cost readily-implementable way to complement existing physical security systems." [4]

While the NMC recognizes the potential for a design basis threat attack, and the hypothetical consequences, this should be counterbalanced with the inherent deterrence and the extremely low probability of such an attack. This reality should be incorporated in the Staff's current rule revision process. *"Deterrence must be consciously integrated into the overall safeguards and security program."* [4]

D. <u>*Security Risk Management*</u>

The underlying principle of security is to put in place adequate countermeasures to meet the foreseeable threats. This assumes the means of making decisions, based on knowledge of the facts, supported by reasonable predictions, and implemented via the process called risk management. Risk management is a broad-based management tool designed to deal with risk in a variety of business and government environments [5]. For security planning, it implies a holistic approach that considers the entire range of security countermeasures. As such, risk management has recently been adopted by the US Department of Defense (and various

government agencies) for planning security protection programs and systems [6, 7, 8]. This is a major change from "total risk elimination" to dealing with only those risks possessing a high probability of occurrence. "The new security world does risk management rather then total risk avoidance" [9]. Security risk management is a critical component to creating effective regulations. NMC believes that risk management concepts should apply equally to security for commercial nuclear power plants. However, the Staff's current revision process does not appear to be based on security risk management concepts.

2. Clarification of "Radiological Sabotage."

A. *Background*

A clear and objective definition of radiological sabotage is essential in order to evaluate and measure the effectiveness of security's protective strategy. The primary goal of the protective strategy is, of course, the prevention of radiological sabotage. Protective strategy performance cannot be objectively measured against an undefined and subjective goal. Currently, the industry's understanding of radiological sabotage is:

> "*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*)."
> (NUREG 1178, page 4-1).

To provide a "margin of safety," NUREG 1178 also states in its analysis assumptions that: *"Any transient or event that causes significant core damage will result in an attendant 10 CFR 100 release*" (page ix). As such, "significant core damage," has been the basis for the industry's protection strategy, target set development, and the NRR's OSRE activities for the last 10 years.

Nonetheless, the Staff now insists that the industry-developed Safeguards Performance Assessment program (SPA) and the revised security Rule "clarify" the meaning of radiological sabotage by inserting Critical Safety Function (CSF) "performance criteria." When considering the CSF criteria the Staff uses for defining "radiological sabotage," it begs for a quantitative limit to which, if exceeded, constitutes "radiological sabotage." This quantitative limit would be used to generate a site-specific set of targets, which if destroyed, would constitute "radiological sabotage." This is similar to the use of dose projections when creating site specific emergency action levels currently in place at each facility. This would be in keeping with the statement, "that are consistent with criteria used in other areas of nuclear power plant regulation," contained in SECY-00-0063.

B. NMC Contentions with Using CSF

NMC disagrees with using CSF criteria as the design basis for protective strategy because it:

- Is too prescriptive and therefore without precedence with regards to CFR rulemaking.

- Is inconsistent with OSRE experience and NUREG 1178 where "significant core damage" is the overarching design basis. By definition, and industry regulatory experience, "significant core damage" requires that all elements of a target set must be compromised or lost in order to initiate an event that may result in a radiological release. Without core damage, there is no radiological risk to public health and safety. CSF usage would result in an ambiguous standard of protection. Core damage is a clearer standard for evaluation of success of plant response to a security attack. The lack of clarity of the significance to public health and safety would likely decrease public confidence in the plants' security response.

- Would require a Back-fit Analysis because it would significantly change the bases for the nuclear industry's security programs and systems (target analysis, vital areas, protective strategy, barrier/delays, training program, etc).

- Would require an unrealistic and unreasonable margin of safety. Again, the loss of a single CSF does not necessarily result in core damage, a 10 CFR Part 100 release, or the release of any radiation. "Significant core damage" is quantifiable, while CSF criteria are not.

- Would result in subjective and inconsistent enforcement. Inclusion of the CSF concept in regulations will serve to create opportunities to cite licensees for limited failures to protect equipment even when that loss may be part of a planned protective strategy. Use of the current Significance Determination Process (which includes the CSF protective concept) has already established a clear disconnect between NRC regional inspectors and NRR (Quad Cities OSRE). Non-risk significant violations unnecessarily erode public confidence and waste NRC and industry resources.

- Would invalidate all facilities' current target sets and development methodologies. All sites' protective strategies (based on a target analysis) have already been tested by the OSRE program. CSF usage would also contradict SECY-00-0063 where it states "overall site security and the security's readiness to respond to an adversary attack were tested and confirmed during regional inspection activity and OSREs."

- The use of "performance" verses "design" criteria is used interchangeably throughout the document and confuses the definition of "radiological sabotage".

- Provides one methodology for arriving at a basis for developing protective strategy. Again, it does not clarify or define radiological sabotage, and it does not provide a mechanism for measuring performance. Instead, "radiological sabotage" would become even more subjective and uncertain.

C. Alternative use for CSF Concept

In performing a target analysis, CSFs are often the top-tree events in PSA/PRA "sabotage fault tree" diagrams and models. The top fault-tree diagram event, however, is "significant core damage" (which, as a margin of safety, is *assumed* to cause a Part 100 release). NMC therefore recommends that the CSF concept instead be published in a Reg. Guide as one methodology for validating targets or performing a target analysis and to, ultimately, develop a sound, target-set based protective strategy. However, the over-arching and "top tree" event (and protective strategy basis) should be changed to "significant core damage" as delineated in NUREG 1178 (and validated through regional inspection activity and OSRE experience).

3. Industry-Developed Self-Assessment Program
(now referred to as "Safeguards Performance Assessment" – SPA)

Before the Staff will endorse the industry-developed SPA, they are insisting that:

- All nuclear sites commit to the SPA in their Licensee Security Plan.
- The industry replaces "significant core damage" with "Critical Safety Functions" (CSF).

NMC disagrees with the Staff's stipulation that sites must commit to the SPA in the security plan. First, the SPA is a "pilot" program. During its trial period, it is likely to be revised. Each revision may require subsequent security plan changes. Instead, each site should submit a letter of commitment to the NRC. Secondly, all sites making simultaneous security plan changes will be an administrative burden on the sites (and NRC). Third, and most importantly, until NMC receives relief of current regulations that do not add to security (generic 50.90/excemption requests recently submitted by Texas Utilities and Commonwealth Edison), we view the addition of the SPA as a significant burden on existing security resources.

In summary, NMC believes that:

- Using Critical Safety Functions would entail numerous problems, as indicated above.

- The Staff should first revise the NRC Baseline Inspection procedure to fit with the final SPA program.

- The Staff should revise the Significance Determination Process (SDP) to mesh with the SPA program and "significant core damage" as security's threshold for "radiological sabotage."

References:

1 - Beck, A., Willis, A. (1995) *Crime and Security*, Perpetuity Press Limited, Leicester, page 181

2 - Brown, B.B. and Altman, I. (1983) 'Territoriality, Defensible Space': An Environmental Analysis' in *Journal of Environmental Psychology*, 3, 203-220,

3 - ACCPA (1999) 'What is Crime Prevention Through Environmental Design?,' http://www.ualberta.ca/ACCPA/cpted.htm

4 – The BDM Corporation (1981) Development of Deterrence Strategies: Prepared for Department of Energy Office of Safeguards and Security

5 - Topping, P. (1997) 'A New Era', *Money Matters* magazine, November:1-3

6 - US CIA (Central Intelligence Agency) (1994) 'Redefining Security', *A Report to the Secretary of Defense and the Director of Central Intelligence*:1-9

7 - US CIA (1997) 'Analytical Risk Management', *DoD Security Awareness Bulletin*, March:23-26

8 - US DoD (Department of Defense) (1997) 'Risk Management and Security Education', *US DoD Security Awareness Bulletin*, March:1-2

9 – Howell, G. (1997) 'The Challenges of Risk Management', *US DoD Security Awareness Bulletin*, March:3-4