DOCKET NUMBER
PROPOSED RULE PR 73
(65FR36649)

(8)

'00 AUG 25 P1:39

August 23, 2000

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

SUBJECT: Federal Register Notice Vol. 65, No. 112, 36649, June 9, 2000
Staff Re-evaluation of Power Reactor Physical Protection Regulation and Position on Definition of Radiological Sabotage
Comments

Dear Sir:

Attached are comments to the subject Federal Register Notice. Periodic evaluation of the rules concerning security at nuclear power reactors is necessary to assure optimum protection of the public health and safety. Fact based, risk informed regulation in this area is welcome.

The Quality of NRC rules is dependent on the information provided to the Staff and to the Commission. During the period since 10CFR73.55 was first published, the NRC rules supporting 10CFR73.55 have changed. Additionally, the Staff has developed significant amounts of important information from inspections, from licensees, and from other Government agencies. The opportunity to apply this information in a logical, straightforward, public manner should improve the rules and the protection of the public health and safety. Other aspects of the review should lead to elimination of conflicting issues, improved inspection guidance and better understanding of the requirements by the industry and the public.

Sincerely,

Douglas R. Kunze

Template = SECY-067

SECY-02

STAFF RE-EVALUATION OF POWER REATOR PHYSICAL PROTECTION REGULATION AND POSITION ON A DEFINITION OF RADIOLOGICAL SABOTAGE

As published in Federal register Vol. 65, No. 112, 36649, dated June 9, 2000

COMMENTS

The referenced Federal Register Notice requests public comment on key issues contained in the Federal Register Notice, including:

1. Revision of 10CFR73.55
2. Clarification of the definition of 'Radiological Sabotage"

The following are comments respectfully submitted for consideration.

1.0 REVISION OF 10CFR73.55 REQUIREMENTS

1.1 Design Basis Threat

When 10CFR Part 73 was first published, it was based on a defined Design Basis Threat, which was made a part of 10CFR73. The threat was, and still is, stated in generic terms and based on classified data. Public comments by individuals in Government positions appear to indicate that the classified data has changed little over the years. Such comments include testimony before Congress.

In March 1993, Dr. Bruce Hoffman of the RAND Corporation testified before the U. S. Senate Committee on Environmental and Public Works, Subcommittee on Clean Air and Nuclear Regulation. In his testimony, Dr. Hoffman stated that "(i)t is difficult to render a conclusive assessment of the threat to commercial nuclear power plants or the security of nuclear systems because no viable attack against such facilities has yet occurred and there

are no lessons to be drawn from past experience." Dr. Hoffman goes on to say "(n)or have there been any credible threats from terrorists or other adversaries against nuclear power plants." He concludes that the "possibility of future terrorist attacks on a commercial nuclear power plant are speculative."

It should be noted in Dr. Hoffman's testimony, he stated that the "frequency of various types of terrorist attacks decrease in direct proportion to the complexity or sophistication required." Security at nuclear power plants is high, and an attack by a terrorist organization would require a great deal of sophistication on the part of the terrorist to be successful. Dr. Hoffman states that "(s)tate sponsorship, in particular, could provide terrorists with the incentives, capabilities and resources . . . for undertaking an ambitious operation." By "state sponsorship" it appears that Dr. Hoffman meant "enemies of the state" which are covered in 10CFR50.13. No other commercial entity is required to defend against state sponsored terrorism.

During the same hearings, Mr. Harry B. Brandon, III, Deputy Assistant Director, Intelligence Division, Federal Bureau of Investigation also presented testimony. Mr. Brandon indicated that "it is the FBI's assessment that the requirements for such an event (sabotage to an NPP) would include extensive coordination, substantial material acquisition, and accurate intelligence gathering – activities which can be susceptible to detection by the FBI and other agencies responsible for counter terrorism."

Mr. Brandon went on to indicate that "the FBI is not in receipt of any credible intelligence indicating that any domestic or international terrorist group is interested in specifically targeting nuclear power plants and/or nuclear fuel facilities." In closing, he indicated that "while the potential for a terrorist group to target a nuclear power station, here or abroad, remains low, . . . the FBI remains committed to a policy of vigilance and cooperation . . . which means that the United States will remain an extremely hostile environment for terrorist activities..."

TIP 33, Nuclear Plant Security, notes that the DBT was revised to include a vehicle bomb. After the April 1995 bombing of the Murrah building in Oklahoma City, the NRC found that there "was still an adequate protective measure" in place at power reactors.

The data supporting the Design Basis Threat as noted remains classified and not readily available to the industry. Such data would be invaluable to the industry in refining and improving the efficiency of its security programs.

The nuclear power industry is an integral part of the electric power infrastructure of the U.S., producing as much as 22% of the nation's electricity. Two recent Presidential documents, Executive Order 13130, and Presidential Decision Directive 63 establish a mechanism to share threat data with the industry. This mechanism is the National Infrastructure Assurance Council. It is recommended that the USNRC sponsor a joint session with the industry before this body to share data affecting the USNRC Design Basis Threat.

The sharing of data and the better understanding of the threat should form the foundation for any potential revisions to 10CRF73.55.

0.1.1 Operational Safeguards Response Evaluation (OSRE)

Over the recent past, the OSRE program has introduced, by inspection, characteristics of the Design Basis Threat that are new, unique and escalating. A major issue with the conduct of the OSRE is the "evolution" of the adversary characteristics and tactics. Each OSRE has been more sophisticated, building on the experience gained at the last site. Each OSRE has upped the adversary's attributes, and given the licensee less credit for the level of hardening applied to the NPP. The current degree of sophistication of the OSRE "adversary" has increased well past the point that a "state sponsored" aggressor would be able to achieve. In looking at the composition of the OSRE "adversary" unit, it mimics a

"state sponsored" adversary in that it has available weapons, tactics, training, and funding normally associated with the best "state sponsored" adversary.

Such "experience" would not be available, even to the most sophisticated adversary. An adversary would not have the opportunity to go through "dress rehearsals' like the OSRE has. Additionally, the postulated sophistication of the adversary (Navy Seal, Army Delta Force or Ranger, or Marine Expeditionary force training) would most likely require significant funding, characteristic of "state sponsorship." State sponsorship would put the adversary in the category of "enemy of the government." 10CFR50.13 states in part that the licensee "is not required to provide design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U. S. defense activities."

The original intent of the RER program, and its successor, the OSRE program, was to measure how well the industry was interpreting the Rules published by the NRC, how well the NRC inspection program was accomplishing it's mission, and how well the NRC's rules were protecting the public health and safety. In other words, the RER and OSRE programs are the NRC's Quality Assurance feedback mechanism for the application of security at NPPs. A consistent application of the measuring tool by the RER program provided significant information to the NRC for consideration in its inspection and rulemaking programs. This RER information lead to improvements in the inspection program, improvements in rulemaking, and most notably, improvements in the industry's security programs. As noted above, the OSRE has applied differing measurement tools at the reactor sites evaluated. Thus, the information gathered by the OSRE might not provide indications of how well the industry is protecting the public health and safety. Additionally, the information can not adequately identify inconsistencies in application of the rules, nor can it provide the necessary evidence of

root causes of short falls. Identification of root cause is very important in correcting any short fall.

The current activities of the OSRE remind one of the comments regarding the Regional inspection process made years ago. The heart of the comments went to inconsistency between Regions, and between inspectors. Additionally, the comments went to regulation by inspection. That is to say, licensees were subject to requirements based only on an individual inspector's interpretations, and in some cases, wishes. The Commission and its Staff worked hard to overcome this reputation and credibility sapping situation.

A major source of information, industry self-assessment programs, is not fully utilized. Currently, self-assessment programs have been applied at several operating reactors, but not all. The existing programs may measure differing performance parameters. By allowing the development of an industry wide, consistently applied, known measurement tool, the NRC could obtain better, more informative feedback regarding security.

0.2 Drills and Exercises

0.2.1 New Subsection

As part of the revisions to 10CFR73.55, SECY-99-241 proposes the creation of a new subsection requiring periodic drills and exercises. Currently 10CFR73.55(b)(4) requires the licensee to "demonstrate the ability of the physical security personnel to carry out their assigned duties and responsibilities." In its INTRODUCTION, Appendix C to 10CFR Part 73 notes that the "safeguards contingency plan is intended to be complimentary to any emergency plans developed pursuant to appendix E of part 50 ...of this chapter."

The above referenced paragraphs appear to require periodic drills and exercises by the security force. The addition of a new subsection would be redundant.

0.2.2 Costs Associated with The Rulemaking

The estimated financial resources applied to security by the industry are presented for illustration purposes and comparison to staff estimates only.

In the Rulemaking Plan, it is noted that the OSRE will "be scheduled to continue until the exercise rule is published in final form." Option 1 states a schedule of 21 months and Option 2 states a schedule of 2 years for the exercise rule. A third option is presented allowing for industry development of a pilot program of exercises and drills. Each option notes the resources required, and in two of the cases notes the resource requirement as a disadvantage.

Given the importance of the contemplated actions, how is the redirection of FTE's considered a "disadvantage?" Security at nuclear power plants is costing the industry in excess of $300 Million per year. In addition to yearly costs, the industry has invested over $1 Billion in security infrastructure (Systems, barriers, etc). The contemplated actions designed to result in changes to 10CFR73.55, the industry's basis for these expenditures, could significantly impact the industry and its ratepayers.

The Rulemaking Plan notes that "licensee resource requirements for this program are estimated to be between $50,000 and $75,000 a year per site." Using the OSRE inspections recently conducted as a yardstick, the actual costs to a single licensee may approach $1 Million. The cost associated with sustaining an OSRE inspection has consistently risen over the period the OSRE has been conducted. In the early stages, the OSRE might have cost the licensee under $100,000. Mid-term costs may have been in the $250,00 range. Over the end game period, costs in the range of $500,000 or more have been reported. A recent OSRE is rumored to have cost the licensee over $1 Million in preparation costs. "Failing" an OSRE is significantly more costly, with impact on licensees rising to as much as $4 Million for preparation costs.

1.4 Backfit

Potential changes to the rules founded on changes in the bases for the rules would require an analysis to determine the potential cost of the changes and the potential benefits to safety of the changes. Changes in the rule may have consequences that may not be readily apparent to the staff. These hidden costs must be accounted for in determining the potential cost associated with the change. It is recommended that the industry work with the staff to provide input to the cost estimates.

2.0 DEFINITION OF RADIOLOGICAL SABOTAGE

A significant accident and sabotage are analogous events in that they both result in a release of radioactivity. The systems used to mitigate an accident are also available to mitigate an act of sabotage. In the "Report of the Working Group to Improve Vital Area Determination Techniques." The report notes that a "reasoned and more appropriate approach may be a best estimate analysis of plant response, with credit for operator actions, to ensure that safety limits are not exceeded." Operator action and other design features should be considered in any sabotage event.

Application of 10 CFR Part 100 has been the basis for the definition of radiological sabotage since 10CFR73 was first published. The USNRC initiated research by and assistance from SANDIA early on (late 1970's) in dealing with this issue. SANDIA and the USNRC developed a set of "Analysis Assumptions" with the first assumption being "(a) 10CFR Part 100 release is the successful sabotage criteria." Subsequently, the USNRC spent several million dollars at Los Alamos National Laboratories for implementation of the analysis of vital equipment and areas at nuclear power reactors in the US. The result of the LANL effort was the concept of "cut sets" of vital areas to be protected.

In 1983, the USNRC established a working group to review vital areas. The "Report of the Working Group to Improve Vital Area Determination Techniques," noted that this systematic analysis of nuclear power plants has lead to identification of areas in "which sabotage actions could result in radiological releases in excess of 10 CFR Part 100 limits." In detailed discussion of the modeling assumptions, the report noted that "(t)he analysis is limited to radiological sabotage mechanisms expected to have consequences exceeding the limits of 10 CFR 100.11(2)."

In its report to Congress regarding FY1985 activities, the USNRC noted the activities of the Regulatory Effectiveness Review (RER) program. In its report the USNRC points to the continuing effort of LANL to identify areas "in which sabotage actions could result in radiological release in excess of 10 CFR 100 limits."

In August 1999, the OSRE team was provided guidance on "radiological sabotage" in the NRC INSPECTION MANUAL, Inspection Procedure 81110, OPERATIONAL SAFEGUARDS RESPONSE EVALUATION (OSRE). Section 81110-03 EVALUATION GUIDANCE, under General Guidance Item c. it is stated that the "team should further assume that a significant radiological release would be the objective of an act of sabotage at a power reactor and should use prevention of significant core damage as an evaluation criterion. This criterion . . . more accurately reflects significant public health and safety concerns." Under Specific Guidance, the team is informed that they "may incorporate operator actions in evaluation of the success of the scenarios."

It is recommended that the USNRC continue to use the criteria of 10 CFR Part 100, which implies significant core damage, in its definition of radiological sabotage. Additionally, it is recommended that the USNRC continue to credit operator actions for mitigation of acts potentially leading to radiological sabotage.

3.0 SUMMARY

It is evident that the nuclear power industry recognizes that security is a requirement of "doing business." Additionally, the industry recognizes the consequences associated with radiological sabotage.

The major issue is not the cessation of security at nuclear power reactors, but the rational, fact and risk based approach to security associated with doing business. The USNRC has recognized the need for risk informed regulation in other important areas. The USNRC has provided the staff with excellent guidance, and the staff in turn has provided significant amounts of guidance regarding the application and content of security programs at power reactors to the industry. The industry has relied on the guidance provided to make significant investments in security.

Current rules and guidance are in need of review, which the staff, as well as the industry, recognizes. Past USNRC sponsored task forces have considered revisions to 10CFR73.55. Redundancy and inconsistencies should be highlighted for elimination. New security techniques and equipment should be taken into consideration, resulting in improved performance oriented, risk based rules. Flexibility in the application of security should be a watchword. What works at one site may not work at another. Results should be the measurement of success.

The current review should be based on feedback obtained from inspections, including RER and OSRE style inspections. A better and more powerful source of feedback is the industry itself. Self-assessment programs, using industry developed standards, should be strongly considered for use by the USNRC. The industry has had significant experience in such programs associated with the safety systems in place at their power reactors. Security related self-assessment programs currently exist at individual power reactor sites. Consistent measurement of activities will allow better decisions by the USNRC, the industry and the public. Consistent, standard measurement is the foundation of the identification of problems and their root causes.

Regarding the Design Basis Threat, the USNRC should assure that the industry has access to appropriate information so that the industry can respond in the most efficient manner possible. Applying rapidly evolving adversary characteristics, on a site-specific basis, is not in the best interests of the USNRC, the industry, or the public. The rapidly evolving characteristics do not allow consistent measurement of security programs, and may mask significant issues at individual power reactors, or potentially, in the industry.

The definition of radiological sabotage has been reviewed many times since the term was first used by the USNRC. Each review appears to have resulted in the same conclusion, that successful radiological sabotage results in significant core damage, and a release in excess of 10CFR100 limits. With this definition, and appropriate feedback on the DBT, the nuclear power industry and the USNRC may continue to protect the public health and safety in an exemplary manner.

The USNRC has asked the staff to undertake a significant project. By using shared data on the DBT, appropriate definitions of radiological sabotage, and the best feedback from inspections and the industry, revisions to the Rules should result in improvement in inspection efficiency and in the efficiency of application of security by the industry. Additionally, the USNRC may retain its role as an excellent regulator, as it has demonstrated since its founding.