



DOCKETED
USNRC

Northern States Power Company
Prairie Island Nuclear Generating Plant
1717 Wakonade Dr. East
Welch, Minnesota 55089

'95 NOV 13 P3:18

OFFICE OF SECRETARY
DOCKETING & SERVICE
BRANCH

November 10, 1995

DOCKET NUMBER
PROPOSED RULE **PR** 60-72,73,75
(60FR42079)
④

Secretary
U S Nuclear Regulatory Commission
Washington, DC 20555-0001

Comments on Proposed Rule Changes - Safeguards for Spent Nuclear Fuel or High-Level Radioactive Waste (60 FR 42079 of August 15, 1995)

Northern States Power Company has reviewed the Federal Register notice of August 15, 1995 referenced above, and would like to offer comments as indicated in Attachment 1 to this letter.

If you have any questions, please direct them to David Axt at 612-388-1121 Extension 4880.

Michael D Wadley
Plant Manager
Prairie Island Nuclear Generating Plant

c: Regional Administrator - Region III, NRC
Senior Resident Inspector, NRC
NRR Project Manager, NRC
J E Silberg

Attachment 1 - Comments to the Nuclear Regulatory Commission from Northern States Power Company - November 10, 1995

9511150068 951011
PDR PR
60 60FR42079 PDR

DS10

**Comments to the Nuclear Regulatory Commission from
Northern States Power Company
November 10, 1995**

Subject: Safeguards for Spent Nuclear Fuel or High-Level Radioactive Waste (60 FR 42079 of August 15, 1995)

Issue #1: No Credible Target-Threat Association for ISFSIs

When considering basic security risk assessment methodology, a target must be credible before it can be linked to a corresponding threat. With regards to sabotage, a target is unattractive unless the sabotage act can produce undesired consequences. For nuclear power plants, these undesired consequences are codified as a 10 CFR, Part 100 release, resulting from radiological sabotage. On the other hand, sabotage scenarios and consequence analyses commissioned by the NRC and other organizations, to date, conclude that a Part 100 release from an ISFSI dry cask system is highly improbable and quantitatively not feasible.

In the NRC's Part 72 Proposed Rule Making of May 31, 1989 it does, however, state that:

... consequence modeling assumptions more severe. . . are possible if unconstrained sabotage resources or protracted loss of control of the storage site are allowed.

Such an act, however, would require an enormous amount of time, tools, equipment and several saboteurs. Even if such a scenario were successfully carried out, the saboteur would still not achieve a Part 100 release. It is therefore reasonable to conclude that ISFSI casks should be afforded protection commensurate with the target sabotage consequences and threat (or lack thereof).

According to a former Sandia National Laboratories employee, who personally oversaw penetration tests of dry casks, there are two plausible sabotage scenarios which could breach an ISFSI cask (given *unconstrained sabotage resources* and a *protracted* time period). One scenario involves explosives; however, the particular explosive package is:

- Extremely difficult to set-up
- Would take a combined total of approximately 130 lbs of explosives & projectile
- Must be positioned, leveled and aimed precisely
- Must be fired from the optimum distance

- Will miss a target the size of a standard cask about 80% of the time

In the second scenario, the saboteur would need a specific type of military oxygen torch. This particular torch system is, however, accessible only to a distinct military organization, and it would require the saboteur to be exposed to the potential radiological release as well as the tremendous heat given off by the oxygen torch.

Nonetheless, the saboteur in both scenarios would still not achieve a Part 100 release.

Issue #2: Use of Deadly Force Contradiction

Security Officers are justified in using deadly force in order to protect the public against radiological sabotage (Part 100 release) by the design basis threat. This is justifiable. There is linkage between sabotage consequences and potential threats. On the other hand, NRC doctrine (verbally communicated) is that security personnel are *not required* to use deadly force in protecting an ISFSI cask. This would seem to indicate a Part 100 release -- the basis for 10 CFR Part 73 security criteria -- is not feasible by sabotaging an ISFSI cask. This contradiction, in and of itself, would indicate that the application of Part 73 level security is duplicitous and indeed excessive.

Issue #3: NRC Security Inspection Burden

NRC inspection efforts for nuclear reactor sites are manpower intensive. If ISFSI security licensing criteria parallel a nuclear site (10 CFR Part 73) then, from an inspection standpoint, the licensing of an off-site ISFSI or an ISFSI in the owner controlled area (OCA) is analogous to creating several new nuclear power plants. Like most of the private sector, the NRC faces manpower cut-backs and shrinking resources. Notwithstanding the rationale of Issues 1 and 2 above, how then will the NRC handle the increased inspection efforts imposed by the additional ISFSIs?

Summary

The absence of a credible target-threat combination for ISFSI dry cask systems ignores basic fundamental vulnerability assessment rationale. The proposed amendments to part 73.51 which specify safeguard requirements for ISFSIs are categorically excessive. Dry casks cannot realistically be stolen, maligned or sabotaged in any way which would produce a 10 CFR Part 100 release. The correlation of reactor and ISFSI site security criteria is baseless and would therefore result in unnecessary licensee expenditures.

Responses to Specific Proposed Rule Questions

1. *Would the proposed amendments impose any significant additional costs for safeguards of currently stored spent nuclear fuel beyond what is now incurred for that purpose?*

Response: Yes. For ISFSIs located outside of a licensee's owner controlled area (OCA), the licensee would need to provide two (2) watchpersons around the clock.

This is approximately 20,000 man-hours a year. Depending on the LLEA agreement, the licensee may also need to provide a dedicated response force which is appendix "B" trained and certified.

2. *Is there reason to expect the costs to future licensees to differ substantially from those of current licensees?*

Response: Yes, for those facilities which might be required to re-locate their ISFSIs to outside their OCA. The costs would increase for reasons stated in question #1 above.

3. N/A.

4. *Are the costs justified by the benefits that would be afforded by the proposed amendments? Are there alternatives that would afford essentially the same benefits, but be more cost effective?*

Response: No, the costs are not justified; the benefits are excessive and unnecessary for those reasons stated in Issues 1, 2 & 3, above. Yes. One alternative would require that the NRC: (1) not lump all spent nuclear fuel storage facilities together, mandating one blanket set of security criteria, (2) develop physical protection criteria which is tailored for the threat-target combination. For dry cask storage facilities, see the attached recommended ISFSI Physical Protection Alternatives.

5. N/A.

ISFSI Physical Protection Alternatives

NEW 7.51 REQUIREMENTS	ALTERNATIVE	RATIONAL
1. Two physical barriers: protected area perimeter fence, defined by 73.2, with isolation zone & the cask itself as second barrier	Two physical barriers: perimeter, nuisance fence with posted "No Trespassing" signs, with locked access.	The level of protection offered by a protected area and isolation zone perimeter fence does not correspond with the target-threat combination; the protection it does provide is negligible
2. Illumination around protected area perimeter	Illumination just around the casks (along with intrusion detection & CCTV)	same as above
3. Complete protected area perimeter intrusion detection system	see above	same as above
4. Random patrols not less than every 8 hours	Random patrols only by LLEA or authorized security personnel.	With CCTV and detection system directly enveloping the casks, and no credible threat, deterrence value of patrols is negligible
5. Security organization; two watchpersons per shift for monitoring detection equipment	No dedicated security organization required, other than random patrols or other security personnel.	Target-threat combination does not support costs associated with a dedicated security organization
6. Documented liaison with designated response force or LLEA	None	N/A
7. Specified screening before granting unescorted access	None	N/A
8. Controlled ID & lock system	None	N/A
9. Escorted individuals under constant escort	None	N/A
10. Redundant communications between security organization & designated response force or LLEA	Not necessary.	Target-threat combination does not support costs
11. Searches of all hand-carried packages and vehicles	Not necessary	With CCTV and detection system directly enveloping the casks, and no credible threat, deterrence value of perimeter search is negligible
12. Written response procedures for unauthorized penetration - including contingencies covered in App.C to part 73	No safeguards response procedures necessary.	Target-threat combination incongruent with Appendix C to part 73
13. All detection and surveillance systems must be tamper-indicating with line supervision -- with comp measures when necessary	None	N/A
14. Security program review every 24 months	At discretion of licensee	Security program not sufficient scope or importance to mandate program review frequency
15. All documentation retained for 3 years	At discretion of licensee	Paperwork reduction. Not necessary