UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SECRETARY

December 17, 2008

COMMISSION VOTING RECORD

DECISION ITEM: SECY-08-0099

TITLE: FINAL RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)

The Commission (with all Commissioners agreeing) approved the final rule as noted in an Affirmation Session and recorded in the Staff Requirements Memorandum (SRM) of December 17, 2008.

This Record contains a summary of voting on this matter together with the individual vote sheets, views and comments of the Commission.

Annette L. Vietti-Cook
Secretary of the Commission

Attachments:
1. Voting Summary
2. Commissioner Vote Sheets

cc: Chairman Klein
Commissioner Jaczko
Commissioner Lyons
Commissioner Svinicki
EDO
OGC

VOTING SUMMARY - SECY-08-0099

RECORDED VOTES

	APRVD	DISAPRVD	ABSTAIN	NOT PARTICIP	COMMENTS	DATE
CHRM. KLEIN	X				X	10/21/08
COMR. JACZKO	X				X	8/22/08
COMR. LYONS	X				X	9/11/08
COMR. SVINICKI	X				X	11/6/08

COMMENT RESOLUTION

In their vote sheets, all Commissioners approved the final rule as noted in an Affirmation Session and reflected in the SRM issued on December 17, 2008.

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: CHAIRMAN KLEIN

SUBJECT: SECY-08-0099 – FINAL RULEMAKING – POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)

Approved XX **Disapproved** _____ **Abstain** _____

Not Participating _____

COMMENTS: **Below** ___ **Attached** XX **None** ___

SIGNATURE

10/21/08

DATE

Entered on "STARS" Yes ✓ **No** ___

Chairman Klein's Comments on SECY-08-0099
Final Rulemaking – Power Reactor Security Requirements

I approve the publication of the final rule, "Power Reactor Security Requirements", in the *Federal Register.* I join my fellow Commissioners in commending staff for their hard work and timeliness on a rule that had significant public involvement. I believe this rule will provide a long-needed update of the Commission's regulations, including the incorporation of numerous post-September 11th enhancements to security and safety. It is clear that these new requirements were well thought out as evidenced by the staff's comprehensive responses to the public comments and thorough explanations of the rule's requirements.

I agree with Commissioner Lyons' vote with the exception of two areas. First, I do not believe that we should require currently-certified designs that undergo amendments to incorporate a more prescriptive design for the central and secondary alarm stations. In my view, currently-certified designs are secure and should not be changed without strong reasons for doing so.

The idea that we should preserve the finality of certified designs is reflected in our Part 52 rules--10 CFR 52.63 permits the Commission to change certified designs through rulemaking only if an analysis shows that change is warranted. But that analysis was not performed by the staff in this rulemaking, nor was the question subject to public notice and comment. Therefore, I cannot support the Commissioner's proposal at this late stage.

While the staff could conceivably be directed to perform the required Part 52 analysis and take additional public comments on the matter, I question whether doing so would be an efficient use of agency resources. Neither the proposed rule nor the regulatory analysis accompanying the final rule identified the proposed CAS/SAS requirement as applicable to already-certified designs, nor has there been any suggestion by my fellow Commissioners that the alarm station configurations in existing certified designs are inadequate. In fact, applicants that select currently-certified designs would be required to maintain the same functions that would be served by a redundant central and secondary alarm station configuration. Imposing a prescriptive design requirement on already-certified designs appears unnecessary. Accordingly, I would oppose further rulemaking proceedings on the issue.

As noted by Commissioner Lyons, several of the requirements are substantially new and beyond those previously required by security orders and must be implemented by current licensees thoughtfully and carefully to ensure that full compliance is achieved and to avoid any unintended consequences. Staff has been working diligently to finalize regulatory guidance by February/March 2009. Staff should make every effort to ensure that this date is met. I differ from Commissioner Lyons only on the time allotted for current power reactor licensees to implement the final rule. I believe allowing current power reactor licensees a 1-year implementation period starting in March 2009, which is the completion date for the regulatory guides, is appropriate. This would provide licensees who may need to make physical changes to a plant during an outage enough time to meet these regulatory requirements. For current reactor licensees, I agree with staff's recommendation that the rule require the submission of a cyber security plan to the NRC for review and approval by way of a license amendment within 180 days of the

effective date of the rule. Also, that the final rule be effective 30 days following the date of publication, which would permit applicability of the rule's requirements to new reactor applicants at the earliest possible date of the rule.

Finally, I have several edits to Enclosure 1, "Federal Register Notice", which are attached.

10/21/08

Chairman Klein's Comments on SECY-08-0099
Final Rulemaking – Power Reactor Security Requirements

I approve the publication of the final rule, "Power Reactor Security Requirements", in the *Federal Register*. I join my fellow Commissioners in commending staff for their hard work and timeliness on a rule that had significant public involvement. I believe this rule will provide a long-needed update of the Commission's regulations, including the incorporation of numerous post-September 11th enhancements to security and safety. It is clear that these new requirements were well thought out as evidenced by the staff's comprehensive responses to the public comments and thorough explanations of the rule's requirements.

I agree with Commissioner Lyons' vote with the exception of two areas. First, I do not believe that we should require currently-certified designs that undergo amendments to incorporate a more prescriptive design for the central and secondary alarm stations. In my view, currently-certified designs are secure and should not be changed without strong reasons for doing so.

The idea that we should preserve the finality of certified designs is reflected in our Part 52 rules--10 CFR 52.63 permits the Commission to change certified designs through rulemaking only if an analysis shows that change is warranted. But that analysis was not performed by the staff in this rulemaking, nor was the question subject to public notice and comment. Therefore, I cannot support the Commissioner's proposal at this late stage.

While the staff could conceivably be directed to perform the required Part 52 analysis and take additional public comments on the matter, I question whether doing so would be an efficient use of agency resources. Neither the proposed rule nor the regulatory analysis accompanying the final rule identified the proposed CAS/SAS requirement as applicable to already-certified designs, nor has there been any suggestion by my fellow Commissioners that the alarm station configurations in existing certified designs are inadequate. In fact, applicants that select currently-certified designs would be required to maintain the same functions that would be served by a redundant central and secondary alarm station configuration. Imposing a prescriptive design requirement on already-certified designs appears unnecessary. Accordingly, I would oppose further rulemaking proceedings on the issue.

As noted by Commissioner Lyons, several of the requirements are substantially new and beyond those previously required by security orders and must be implemented by current licensees thoughtfully and carefully to ensure that full compliance is achieved and to avoid any unintended consequences. Staff has been working diligently to finalize regulatory guidance by February/March 2009. Staff should make every effort to ensure that this date is met. I differ from Commissioner Lyons only on the time allotted for current power reactor licensees to implement the final rule. I believe allowing current power reactor licensees a 1-year implementation period starting in March 2009, which is the completion date for the regulatory guides, is appropriate. This would provide licensees who may need to make physical changes to a plant during an outage enough time to meet these regulatory requirements. For current reactor licensees, I agree with staff's recommendation that the rule require the submission of a cyber security plan to the NRC for review and approval by way of a license amendment within 180 days of the

effective date of the rule. Also, that the final rule be effective 30 days following the date of publication, which would permit applicability of the rule's requirements to new reactor applicants at the earliest possible date of the rule.

Finally, I have several edits to Enclosure 1, "Federal Register Notice", which are attached.

10/21/08

applicability consistent with the requirements in the final rule § 73.55(m), "Security program reviews." The Commission has determined that such reviews are needed to ensure target sets are complete and accurate at all times.

Section 73.55(g), Access Controls. The Commission received a comment that the proposed § 73.55(g) does not close a dangerous loophole in current search requirements for law enforcement personnel and security officers which allows bona fide Federal, State, and local law enforcement personnel on official duty and licensee security personnel who have exited the protected area (PA) to reenter the PA without being searched for firearms. The commenter argued that such exceptions could provide insiders or corrupt law enforcement personnel collaborating with adversaries with significant opportunities to introduce contraband, silencers, ammunition, or other unauthorized equipment that could be used in an attack. The commenter stated that this practice should be explicitly forbidden in the rules except under extraordinary circumstances. The Commission disagrees with this comment. On-duty law enforcement personnel ~~are~~ may be granted access by licensees when there is a need for such access and are escorted while inside the PA. ~~In addition, the NRC has no basis for assuming, nor has the commenter supplied one, that law enforcement personnel pose an insider threat.~~ With respect to licensee security personnel, they are searched for firearms, explosives, and incendiary devices upon reporting for duty and are under the observation of other security personnel who are subject to the licensee's continuous behavioral observation program when performing duties. Upon assuming their duties, armed security officers must continue to be subject to the search criteria for explosives and incendiary devices upon re-entry to the PA. Both law enforcement personnel and licensee armed security personnel have been determined, through rigorous background investigations, to be trustworthy and reliable before being issued a firearm as part of their assigned duties. The Commission concluded that this exception to the required search criteria is necessary and appropriate to avoid unnecessary regulatory burden associated with these operating conditions.

requires that the licensee will control passwords/passcodes used for security computers, electronic systems, or secured areas.

Section 73.55(g)(7)(i)(F) is added to require the licensee to deny access (escorted or unescorted) to any individual for whom access is currently denied at another NRC-licensed nuclear power reactor facility.

The Commission received several comments that the requirements described in proposed § 73.55(g)(7)(ii) regarding the specific information to be included on photo-identification badges issued to non-employee personnel who require frequent or extended unescorted access to a facility are an unnecessary regulatory burden. The Commission agrees in part, and § 73.55(g)(7)(ii) is revised to retain only the requirement for badges to visually reflect that the individual is a non-employee and that no escort is required. The proposed §§ 73.55(g)(7)(ii)(B) through (D) are deleted. The Commission's expectation is for licensees to electronically record the individual's access level, period of unescorted access, and employer within security databases. The Commission concluded that current badge technology is predicated upon computerized access control methodologies that store much of this information electronically on badges or keycards and in associated databases. Therefore, the need to visually display such information on badges is unnecessary. The proposed § 73.55(g)(7)(ii)(E) requirement for the designation of assigned assembly areas on badges is also deleted as it is determined to be an unnecessary regulatory burden.

The Commission received a comment to clarify the proposed § 73.55(g)(8) relative to the training of personnel assigned to perform escort duties. The rule requires that all escorts will be trained to perform escort duties and that this training may be accomplished through existing processes such as the General Employee Training (personnel escort) and/or the security Training and Qualification Plan (vehicle escorts). This training requirement ensures that any individual assigned to escort duties understands their responsibilities and the activities the

of which must be protected in accordance with the requirements of the central alarm station within this section.

(3) The licensee's intrusion detection and assessment systems must be designed to:

(i) Provide visual and audible annunciation of the alarm.

(ii) Provide a visual display from which assessment of the detected activity can be made.

(iii) Ensure that annunciation of an alarm indicates the type and location of the alarm.

(iv) Ensure that alarm devices to include transmission lines to annunciators are tamper indicating and self-checking.

(v) Provide an automatic indication when the alarm system or a component of the alarm system fails, or when the system is operating on the backup power supply.

(vi) Support the initiation of a timely response in accordance with the security plans, licensee protective strategy, and associated implementing procedures.

(vii) Ensure intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.

(4) Alarm stations.

(i) Both alarm stations required by paragraph (i)(2) of this section must be designed and equipped to ensure that a single act, in accordance with the design basis threat of radiological sabotage defined in § 73.1(a)(1), cannot disable both alarm stations. The licensee shall ensure the survivability of at least one alarm station to maintain the ability to perform the following functions:

(A) Detect and assess alarms;

(B) Initiate and coordinate an adequate response to an alarm;

(C) Summon offsite assistance; and

(D) Provide command and control.

(5) Non-portable communications equipment must remain operable from independent power sources in the event of the loss of normal power.

(6) The licensee shall identify site areas where communication could be interrupted or cannot be maintained, and shall establish alternative communication measures or otherwise account for these areas in implementing procedures.

(k) Response requirements.

(1) The licensee shall establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats up to and including the design basis threat of radiological sabotage as defined in § 73.1, to prevent significant core damage and spent fuel sabotage.

(2) The licensee shall ensure that all firearms, ammunition and equipment necessary to implement the site security plans and protective strategy are in sufficient supply, are in working condition, and are readily available for use.

(3) The licensee shall train each armed member of the security organization to prevent or impede attempted acts of ~~theft or~~ radiological sabotage by using force sufficient to counter the force directed at that person, including the use of deadly force when the armed member of the security organization has a reasonable belief that the use of deadly force is necessary in self-defense or in the defense of others, or any other circumstances as authorized by applicable State or Federal law.

(4) The licensee shall provide armed response personnel consisting of armed responders which may be augmented with armed security officers to carry out armed response duties within predetermined time lines specified by the site protective strategy.

(5) Armed responders.

(i) The licensee shall determine the minimum number of armed responders necessary to satisfy the design requirements of § 73.55(b) and implement the protective strategy. The

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

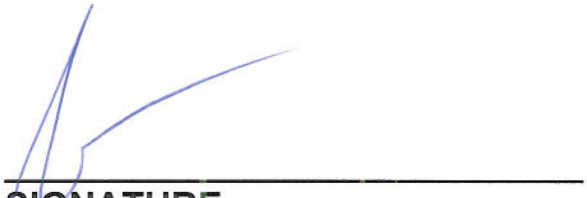
FROM: Commissioner Gregory B. Jaczko

SUBJECT: SECY-08-0099 – FINAL RULEMAKING – POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)

Approved __X__ Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below ___ Attached _X_ None ___



SIGNATURE

8/22/09

DATE

Entered on "STARS" Yes _X_ No ___

Commissioner Jaczko's Comments on SECY-08-0099
Final Rulemaking – Power Reactor Security Requirements

I approve of the final rule package subject to my general comments and my specific comments on the staff resolution of public comments.

Overall, I compliment the staff for the hard work that it has done to present this rulemaking to the Commission. I also acknowledge the effort made by the staff to accelerate the completion of the rule package to the Commission. I am also appreciative of the public and all the stakeholders for their extensive involvement and interaction in the rulemaking process.

I have made every effort to complete my review in a timely manner. With the vast amount of information and with the extreme importance of the content, reviewing this rule in approximately one month was a challenge. In the future, the staff should consider mechanisms to facilitate greater Commission understanding of the content and the staff's resolution of comments on behalf of the Commission to facilitate a more timely review by the Commission. Reading, comprehending, debating and deciding on years' worth of effort in thousands of pages of rule text and supporting documents is a challenging task. I encourage the staff to consider mechanisms to provide the information in the final rule in more papers to allow the Commission to consider the rule over a longer period without extending the final completion deadline. For example, the provisions in 50.54(hh) could have been provided to the Commission for review and approval separately from the provisions modifying 73.55. The entire package would then be affirmed once all the sections were reviewed.

The following are general comments about the rule as a whole. Some of these comments are reflected in my specific views are the staff's resolution of public comments.

I fundamentally disagree with the approach the staff has taken with regard to the force on force exercises observed by the Nuclear Regulatory Commission and required by the Energy Policy Act of 2005. I believe the staff should specify within the rule the requirement for the licensees to participate in NRC observed force on force exercises every three years. The rule should further describe the basic requirements and elements of the program. Since many of the details of the program's implementation remain licensee responsibilities, it is appropriate to specify the program in the rule. For example, the industry currently provides the adversary force used for the exercises. The rule makes no mention of the responsibility of licensees in regard to the adversary force. In fact, the staff provides significant regulatory detail about the force on force exercises the licensees are required to conduct, but the staff provides no such description for the exercises licensees are required to conduct if they are observed by the NRC. This appears to be an inconsistency in the rule.

I disagree with the revised final rule that the requirements to design, construct, and equip both the central alarm station (CAS) and secondary alarm station (SAS) to the same standards is only a prudent safety enhancement for future nuclear power plants, but not for existing operating reactors. Specifically, existing nuclear power plants should be required to locate the SAS within a site's protected area, ensure that the SAS is bullet resistant, and limit visibility into the SAS from the perimeter of the protected area as a

matter of enhanced safety, requiring a backfit analysis. I was not able to find such an analysis in the rule package.

I generally supported the staff rule change to not require the review of security plan changes. I only support this change, however, if the commission provides sufficient resources and a strong commitment to fully inspect the security plans by expanding the baseline inspection program.

The staff should clarify how part 73.55(a)(6) applies to amended design certifications. Specifically, the staff should add, "or standard design certification amended after **[INSERT EFFECTIVE DATE OF FINAL RULE]**" after "or reference a standard design certification issued after **[INSERT EFFECTIVE DATE OF FINAL RULE]**".

The staff should renumber 73.55(e)(11) to be 73.55(e)(10)(ii) to be consistent with the statements of consideration and the expressed intent therein. This change will ensure that 73.55(e)(10) is a generic requirement to all types of barriers, water and land.

The following are specific comments about the staff response to public comments. (References are to Enclosure 4 to the SECY paper, "Integrated Comment Responses Supporting Final Rule: Power Reactor Security Requirements" in the order in which the comment and staff response appear.) In each case in which I provide comments or deviate from the staff response to the comments, my fellow Commissioners should interpret my modifications to apply as necessary to the rule text and statements of considerations in addition to the specific comment response.

General Issues and Specific Questions

1. agree
2. partially disagree – The rule does in my view accomplish more than codifying existing orders. I do not agree, however, with the staff resolution of the MoX fuel requirements and the incorporation of the security-based drills as required by the Energy Policy Act.
3. agree
4. disagree – The staff should address the commenter's statement about a lack of change in the threat environment. The threat environment is not stable and has changed since 2005.
5. agree
6. agree in general

Regulatory Analysis Issues

1. agree
2. agree
3. agree
4. agree

10 CFR 50.54(hh)

1. agree
2. agree
3. agree
4. agree and disagree -- The licensees should also consider emergency preparedness options that mitigate consequences.
5. agree
6. agree
7. disagree – The licensees should consider pre-positioning some equipment.
8. agree
9. agree
10. agree
11. agree – I do believe, however, that inclusion of communication

challenges in emergency preparedness exercises should be considered by the agency in other rulemaking initiatives.
12. agree (see #11, above)
13. agree and disagree – The staff response should be revised to address spent fuel fires or indicate that spent fuel pools are considered part of the "power reactor facility", the term used in the staff response.
14. disagree – The staff comment should clarify the comment (and rule language) to clarify that "reduce visual discrimination" means "reduce visual discrimination during low-light conditions".
15. agree
16. agree
17. agree
18. disagree – The staff should revise its comments to indicate that extensive engineering analyses of airliner crashes have been conducted.
19. agree
20. agree
21. disagree – I continue to disagree with the agency's approach to dealing with operational programs for the licensing of power reactors under part 52 of the Commission's regulations. This is another example of a weakness of the current approach.

10 CFR 73.54 "Protection of digital computer and communication systems and networks

1. agree
2. agree
3. disagree – The staff appears to *agree* with the comment. The staff should revise accordingly.
4. agree
5. agree and disagree – The staff does not appear to have an implementation timeframe. The plans must be submitted within 180 days, but there does not appear to be a deadline for implementation of the plans.
6. agree
7. agree – The staff should monitor this decision closely. It may ultimately be more effective to place the cybersecurity program within another or standalone organization at a licensed facility.
8. agree
9. agree
10. disagree – The response does not appear to address the comment.
11. agree
12. agree
13. agree – The staff should add to the response that the licensee should use independent experts where possible.
14. agree
15. agree
16. agree
17. agree
18. agree
19. agree
20. agree

10 CFR 73.55

1. agree
2. agree
3. disagree – The rule language should continue to contain definitions for key terms, especially "target set." "Target set" is one of the most important concepts in the force-on-force program and its use should be defined in regulations.
4. agree
5. disagree – The term unauthorized should be defined in 73.2.
6. agree
7. agree in part – The staff should describe the process the agency will use to inspect the security

plan changes made under 50.54(p) absent a requirement to submit and review all security plans.

8. agree in part (see #7 above)
9. agree in part (see #7 above)
10. agree in part (see #7 above)
11. agree
12. agree
13. disagree – The structure of 73.55(b) does appear to create ambiguities about the requirements for meeting the general performance objectives. 73.55(b)(2) and 73.55(b)(3) both specify what the "physical protection program must" accomplish. The staff should clarify how these two requirements relate to each other.
14. agree
15. disagree (see #13 above)
16. agree
17. disagree (see #13 above)
18. agree
19. agree
20. agree
21. agree
22. agree
23. agree
24. agree
25. agree
26. agree
27. agree
28. agree
29. agree
30. agree
31. agree
32. agree
33. agree
34. agree
35. agree
36. agree
37. agree
38. agree
39. agree
40. agree
41. agree
42. agree
43. agree
44. agree
45. agree
46. agree
47. agree
48. agree
49. disagree – The staff should directly answer the commentor's question
50. disagree – The staff should delete the first sentence from the response
51. agree
52. disagree – The staff should also add a comment about the ongoing aircraft security rulemaking for new reactor designs
53. disagree (see #52 above)
54. disagree – The staff should indicated that these issue are being addressed through orders and the new 50.54(hh) section
55. disagree (see #54 above)
56. agree
57. disagree – The staff should also reference the provisions of 50.54(hh), which requires mitigation measures for spent fuel pools.
58. agree
59. agree
60. agree
61. agree
62. agree
63. agree
64. disagree – It is not clear how addressing this issue in guidance will achieve the performance measure intended by the staff and how addressing in guidance will address the commenter's concerns.
65. disagree – The commenter makes a legitimate argument about the desire to have the barriers delineate the area to be protected. Staff should resolve this comment and not simply defer this issue to guidance.
66. disagree – The staff does not reference the design

requirement to address core damage and spent fuel sabotage. The staff should be consistent between 73.55(b) and this section.

67. agree
68. agree – The staff, however, appears to need to restore the "clearly delineate" performance standard for this provision to have regulatory effect.
69. agree
70. agree
71. agree
72. agree
73. agree
74. agree
75. agree
76. agree
77. agree
78. agree
79. agree
80. agree
81. agree
82. agree
83. agree
84. agree
85. agree
86. agree
87. agree
88. agree
89. agree
90. agree
91. agree
92. agree
93. agree
94. agree
95. agree
96. agree
97. agree
98. agree
99. agree
100. agree
101. disagree – This section should be retained. 73.58 requires awareness of security and safety interface activities, but does not require the adjustments and compensatory measures in this section.
102. agree
103. agree
104. agree
105. agree – Subject to a renumbering of 73.55(e)(10)(i) and 73.55(e)(11)
106. agree
107. agree
108. agree
109. agree
110. agree
111. agree
112. agree
113. agree
114. agree
115. agree
116. disagree – The general requirement of 73.55(e)(10) appears to be weaker than 73.55(e)(10)(i)(A). The staff should correct this.
117. agree
118. agree
119. agree
120. agree
121. agree
122. agree
123. agree
124. agree
125. agree
126. agree
127. agree
128. agree
129. agree
130. agree
131. agree
132. agree
133. agree
134. agree
135. disagree – The staff should discuss the fact that the design basis threat is a requirement on licensee personnel to defend the facility without the need for additional response personnel.
136. agree
137. agree
138. agree
139. agree
140. agree
141. agree
142. agree

143. agree
144. agree
145. agree
146. agree
147. agree
148. agree
149. agree
150. agree
151. agree
152. agree
153. agree
154. agree
155. agree
156. agree
157. agree
158. agree
159. disagree
160. agree
161. agree
162. agree
163. agree
164. disagree – The staff should maintain the proposed rule language with the addition of the word "credible". Some information about a threat may not be site specific, but may be general credible threat information.
165. disagree (see #164 above)
166. agree
167. agree
168. agree
169. disagree – The staff should retain some language in 73.55(g)(5) to reflect the requirement that the licensee must still ensure protection against the design basis threat, significant core damage, and spent fuel sabotage.
170. agree
171. agree
172. agree
173. agree
174. agree
175. agree
176. agree
177. agree
178. agree
179. agree
180. agree
181. agree
182. agree
183. agree
184. agree
185. agree
186. agree
187. agree
188. agree
189. agree
190. agree
191. agree
192. agree
193. agree
194. agree
195. agree
196. agree
197. agree
198. agree
199. agree
200. agree
201. agree
202. agree
203. agree
204. disagree – Definitions for important terms should continue to be in the regulation.
205. agree
206. disagree – The commenter raises an interesting issue.
207. see #206 above
208. agree
209. agree
210. agree
211. agree
212. agree
213. agree
214. agree
215. agree
216. agree
217. agree
218. agree
219. agree
220. agree
221. agree
222. agree
223. agree
224. agree
225. disagree – Unauthorized materials should be defined in

73.2 as the staff has defined it in the comment.

226. agree
227. agree
228. agree
229. agree
230. disagree
231. disagree
232. agree
233. agree
234. agree
235. agree
236. agree
237. agree
238. agree
239. agree
240. agree
241. agree
242. agree
243. agree
244. agree
245. agree
246. disagree – It is not clear why the location of the uninterruptable power supply would not be a vital area.
247. agree
248. see previous comments about radiological sabotage and core damage and spent fuel sabotage
249. agree
250. agree
251. agree
252. agree
253. agree
254. agree
255. agree
256. agree
257. agree
258. agree
259. agree
260. agree
261. agree
262. agree
263. agree
264. agree
265. agree
266. agree
267. agree
268. agree
269. agree
270. agree
271. disagree
272. disagree – By definition, no one needs to be trained to recognize "obvious" tampering. Here the security personnel need to be trained to recognize "unobvious" tampering, so the word obvious should not be added.
273. agree
274. agree
275. disagree
276. agree
277. agree
278. agree
279. agree
280. agree
281. agree
282. agree
283. agree
284. agree
285. agree
286. agree
287. agree
288. agree
289. agree
290. agree
291. agree
292. agree
293. agree
294. agree
295. agree
296. agree
297. agree
298. agree
299. agree
300. agree
301. agree
302. agree
303. agree
304. agree
305. agree
306. agree
307. agree
308. agree
309. agree
310. agree
311. agree
312. agree
313. disagree

314. disagree (see #317 below)
315. agree
316. agree
317. disagree – This provision effectively creates a third design basis threat standard, a modified theft and diversion standard. This issue should be addressed in the design basis threat rule. If MOX fuel does not meet the threshold for protection against the theft and diversion design basis threat the new theft and diversion standard should be developed.
318. see #317
319. see #317
320. see #317
321. agree
322. agree
323. agree
324. agree
325. agree
326. agree
327. agree
328. see comments on appendix B
329. see comments on appendix B
330. see comments on appendix B
331. agree
332. agree
333. agree
334. agree
335. agree
336. agree
337. agree
338. agree
339. agree
340. agree
341. agree
342. agree
343. agree
344. agree
345. agree
346. agree
347. agree
348. agree
349. agree
350. agree
351. agree
352. agree
353. disagree
354. agree
355. agree
356. agree

10 CFR 73.56

1. agree
2. disagree
3. agree
4. agree
5. agree
6. agree
7. agree
8. agree
9. agree
10. agree
11. agree
12. agree
13. agree
14. agree
15. agree
16. agree
17. agree
18. agree
19. agree
20. agree
21. agree
22. agree
23. agree
24. agree
25. agree
26. agree
27. agree
28. agree
29. agree
30. agree
31. agree
32. agree
33. agree
34. agree
35. agree
36. agree
37. agree
38. agree
39. agree
40. agree

10 CFR 73.58 Safety/Security Interface Requirements for Nuclear Power Reactors

1. agree
2. agree
3. agree -- It was, however, my understanding from the draft rule that this provision was a reasonable assurance provision.
4. agree
5. agree
6. agree
7. agree
8. agree

Part 73 Appendix B

1. agree
2. agree
3. agree
4. agree
5. agree
6. agree
7. agree
8. agree
9. agree
10. agree
11. agree
12. agree
13. agree
14. agree
15. agree
16. agree
17. agree
18. agree
19. agree
20. agree
21. agree
22. agree
23. agree
24. agree
25. agree
26. agree
27. agree
28. agree
29. agree
30. partially agree (see #34 below)
31. see #34 below
32. see #34 below
33. see #34 below
34. disagree – The Commission should place a requirement on licensees to participate in NRC observed and evaluated force on force exercises in accordance with the Energy Policy Act. While I agree that the licensee administered force on force exercises may be considered part of training, the NRC observed exercise is not. The program should be described in regulations, specifically in 73.55.
35. see #35 above
36. agree
37. agree – I do believe, however, that the Commission should initiate a rulemaking to address this issue.
38. disagree – The NRC should establish the NRC observed force on force program in regulation and establish the requirements on the licensees for their participation. The response that "there are no regulations prohibiting license substitutions of personnel" simply begs this questions. This rulemaking is intended to establish what the regulations should be for the licensees conducting the NRC observed force on force exercises.
39. agree
40. agree
41. agree
42. agree
43. agree
44. agree
45. agree
46. agree
47. agree
48. agree

49. agree
50. agree
51. agree
52. agree
53. agree
54. see comment #35 and #38 above
55. agree
56. agree
57. agree
58. agree
59. agree
60. agree
61. agree
62. agree
63. agree
64. agree
65. agree
66. agree
67. agree
68. agree
69. agree
70. agree
71. agree
72. agree
73. agree
74. agree
75. agree
76. agree
77. agree
78. agree
79. agree

Part 73 Appendix C, Section II

1. agree
2. agree
3. see comments on part 73, Apprendix B
4. agree
5. agree
6. see previous comments with regard to radiological sabotage, significant core damage and spent fuel sabotage
7. agree
8. agree
9. agree
10. agree
11. agree
12. agree
13. agree
14. agree
15. agree
16. agree
17. agree
18. agree
19. agree
20. agree
21. agree
22. agree
23. agree
24. agree
25. agree

8/22/08

Gregory B. Jaczko Date

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER LYONS

SUBJECT: SECY-08-0099 – FINAL RULEMAKING – POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)

Approved __X__ Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below ___ Attached __X__ None ___

Peter B. Lyons
SIGNATURE

9/ 11 /08
DATE

Entered on "STARS" Yes __X__ No ___

Commissioner Lyons' Comments on SECY-08-0099
Final Rulemaking – Power Reactor Security Requirements

I approve the publication of the final rule in the *Federal Register*, as recommended by the staff in SECY-08-0099, and approve certification that this rule, if promulgated, will not have significant impact on a substantial number of small entities, subject to the following comments and modifications.

I join Commissioner Jaczko in commending the staff for its hard work to present this rulemaking to the Commission on an accelerated schedule. I would further commend the staff for an exceedingly thorough and complete effort in responding individually to a total of 559 specific public comments and for a very good public outreach effort.

I support the staff's assertion that the requirements being codified represent a substantial increase in safety, noting that the baseline for this increase was our pre-2001 regulations. I recognize that in addition to codifying requirements similar to the NRC security orders that were issued following the events of September 11, 2001, this rulemaking further adds requirements based on lessons learned during implementation of the security orders and through our inspection and oversight processes. The end result is a rule package that provides an up-to-date regulatory framework for current and any future power reactors.

I support the staff's recommendations and the associated bases and justifications, as modified by the following comments.

Implementation Timeframe

Several of the requirements are substantially new and beyond those previously required by security orders and must be implemented by current licensees thoughtfully and carefully to ensure full compliance is achieved and to avoid any unintended consequences. This level of care will require completion of the requisite regulatory guidance, scheduled for February/March 2009, and then development of the associated site-specific procedures, programs, and processes. For current power reactor licensees, I believe these efforts will reasonably require more than the proposed 180 day implementation period from the effective date of the rule (i.e., 30 days following its publishing). The staff's basis for a 180-day implementation period is that many of the provisions are already in place from the security orders and many of the added requirements can be changed by licensees without NRC approval in accordance with 10 CFR 50.54(p), 50.90, and 73.5. Although I recognize this to be the case, I believe that this implementation period should start from the March 2009 timeframe, when guidance documents should be finalized. I support the other implementation provisions of the rule, such as 180 days to submit a cyber-security plan for staff review and an effective date of 30 days following publication of the rule for new reactor applicants. **Therefore, the staff should change the final rule to require, for current power reactor licensees, a 1-year implementation period from the date of publication of the final rule.**

Petitions

I agree with the staff's resultant disposition of the three petitions associated with this rulemaking. In addition, I strongly affirm my support for the 10 CFR 73.58 safety/security interface requirements within the rule that ensure both safety and security are not adversely affected by changes to the plant or procedures for either. I greatly appreciate the thought and effort that both staff and stakeholders have given this aspect of the rule. Finally, I agree with the

staff's approach that this rule (and rulemaking in general) not become unnecessarily prescriptive.

However, the staff's bases for the two proposals of PRM-73-13 are weak on the following points.

First, the petitioner proposes that visitors who do not yet have sufficient information to be granted unescorted access be kept under armed escort (rather than the currently required unarmed escort) while in the protected area. Staff's denial is based essentially on the fact that there have been no past incidents that call into question the sufficiency of our current requirements. This is a little like saying our most limiting accident design bases are acceptable because none have ever occurred. Therefore, the staff should include in its basis for denial the current applicable requirements and guidance that the staff believes *are* sufficient (e.g., the nature and extent of the information that is currently required to grant escorted access and the responsibilities of the escorts).

The petitioner's other proposal was that when information becomes known that would prevent an individual from gaining unescorted access, the licensee will ensure the individual does not enter the protected area. Staff's denial is based essentially on the fact that the rule defines the information needed to *grant* unescorted access and does not need to further prescribe the information that could preclude such access. This is an appropriate basis. However the staff's assertion that "There is no particular piece of information obtained during a background investigation that would automatically disqualify an individual from access." is unnecessarily overstated. In fact, there certainly can be such information that arises during a background investigation. The staff offers one good example of this in the rule itself: individuals will be denied access if they are currently denied access at another facility. In addition, credible information from law enforcement authorities that indicate an individual's malicious intent toward the facility would clearly be another example.

Therefore, the staff should include in its bases for denials of PRM-73-13 a clearer articulation of the extent of the currently applicable existing requirements and guidance and how they serve to protect against the scenarios inferred or stated by the petitioner. Additionally, staff should clarify text, as appropriate, that could be interpreted as an overstatement.

I will also comment on some of the points raised by Commissioner Jaczko in his notation vote on this paper.

Force-on-Force Exercises

I agree with the staff that we need not codify the statutory requirement in the Energy Policy Act of 2005 that the NRC observe certain Force-on-Force exercises at reactor sites. I have no doubt at all that the NRC will continue, as it has, to fulfill this responsibility to Congress. In addition, the proposed rule in 10 CFR Part 73 Appendix B.IV(C)(3)(I)(1) notes that "Force-on-force exercises conducted to satisfy the NRC triennial evaluation requirement can be used ....." clearly indicates the existence of NRC oversight of these exercises. Furthermore, I am not concerned about difference between this proposed final rule requirement for reactor facilities and the current requirements of 10 CFR 73.46(b)(9) for Category I facilities. The nature of the potential consequences at Category I facilities have historically justified a regulatory treatment that differs in many cases from that imposed on reactors. The NRC oversight of security at Category I facilities is predominate among such examples.

Physical Security Enhancements

I support the physical security enhancement of the rule that requires the Central Alarm Station (CAS) and Secondary Alarm Station (SAS) to have functionally equivalent capabilities such that no single act of radiological sabotage could disable the key functions of both. Furthermore, I support the requirement for an uninteruptible power supply for intrusion detection and assessment equipment at the protected area perimeter that are relied upon to initiate the licensee's protective strategy. I agree with the staff that the secondary alarm station for existing operating reactors need not meet the same standards imposed on the CAS. Staff points out correctly that the existing SAS requirements today meet the regulatory standard of high assurance of adequate protection. Designing and constructing both CAS and SAS to the same requirements for new reactors is a relatively easy enhancement that I support. **I agree with Commissioner Jaczko's comment that staff should clarify this requirement (i.e., 10 CFR 73.55(a)(6)), and I support that it should apply to amended design certifications**.

Vehicle Control Measures

I agree with Commissioner Jaczko's comment that 10 CFR 73.55(e)(11) should be re-numbered as 10 CFR 73.55(e)(10)(ii), subject to rule text changes that accomplish the following: a) clarify that the performance standard for vehicle control measures for both land and waterborne vehicles is to protect against the design basis threat of radiological sabotage, b) to clearly differentiate this standard with requirements that are specific to each vehicle type, and c) to avoid any inconsistency with the DBT language in 10 CFR 73.1(a)(1)(E). Conforming changes, if appropriate, should also be made to the Statements of Consideration and/or other sections of the rule. I note that this renumbering would also be consistent with the staff's response to the 165th public comment under 10 CFR 73.55. Such changes could be similar to the following suggested rule text (strikeouts are suggested deletions and underlined text are suggested additions to staff's proposed final rule):

73.55(e)(10) Vehicle control measures. Consistent with the physical protection program design requirements of § 73.55(b), ~~the licensee shall protect against vehicle use as a means of transporting unauthorized personnel or materials to gain proximity to a protected area or vital area, or otherwise penetrate the protected area perimeter.~~ and in accordance with the site-specific analysis, the licensee shall establish and maintain vehicle control measures, as necessary, to protect against the design basis threat of radiological sabotage vehicle bomb assault.

(i) Land vehicles. Licensees shall:

(A) Design, construct, install, and maintain a vehicle barrier system, to include passive and active barriers, at a stand-off distance adequate to protect personnel, equipment, and systems necessary to prevent significant core damage and spent fuel sabotage against the effects of the design basis threat of radiological sabotage land vehicle bomb assault.

(B) Periodically check the operation of active vehicle barriers and provide a secondary power source, or a means of mechanical or manual operation in the event of a power failure, to ensure that the active barrier can be placed in the denial position to prevent unauthorized vehicle access beyond the required standoff distance.

(C) Provide periodic surveillance and observation of vehicle barriers and barrier systems adequate to detect indications of tampering and degradation or to otherwise ensure that each vehicle barrier and barrier system is able to satisfy the intended function.

(D) Where a site has rail access to the protected area, install a train derailer, remove a section of track, or restrict access to railroad sidings and provide periodic surveillance of these measures.

~~(11)~~ (ii) ~~Waterways. The licensee shall:~~ Waterborne vehicles. Licensees shall:

~~(i) In accordance with the site-specific analysis, establish and maintain waterborne vehicle control measures, as necessary, to protect against the design basis threat of radiological sabotage waterborne vehicle bomb assault.~~

~~(ii)~~ (A) Identify areas from which a waterborne vehicle must be restricted, and where possible, in coordination with local, state, and Federal agencies having jurisdiction over waterway approaches, deploy buoys, markers, or other equipment.

~~(iii)~~ (B) In accordance with the site-specific analysis, provide periodic surveillance and observation of waterway approaches and adjacent areas.

Licensee Incorporation of Changes

I support providing licensees the ability to incorporate some of the rule changes into their security plan through existing regulatory provisions that allow such changes when they do not decrease security plan effectiveness. I would favorably entertain staff requests for additional resources aimed at obtaining the talent and expertise necessary to review cyber-security plans and to inspect the adequacy of their implementation.

Treatment of MOX Fuel Assemblies Prior to Use

On the matter of creating provisions within this rule for additional protection of mixed-oxide (MOX) fuel assemblies from theft and diversion prior to use in a reactor, beyond the requirements imposed on non-MOX power reactor fuel but less than those for formula quantities of strategic special nuclear material, I would agree with Commissioner Jaczko that this creates the appearance of a new category of nuclear material. However, it is a well-defined category with well-defined requirements, so I see no particular problem with its existence. Further, these provisions originated from and remain consistent with the requirements placed on the Catawba MOX lead test (fuel) assemblies. I would certainly be willing to entertain a future staff proposal to remove such special requirements if justified based on our regulatory, technical, and operational experience with MOX fuel.

Public Comments and Staff Responses

On the whole, I believe the staff responses to public comments were adequate to document that each comment was thoughtfully considered. As noted above, I commend the staff for what appears to be a herculean effort in individually responding to the 559 public comments given the accelerated schedule. However, I will comment on the following staff responses identified in Commissioner Jaczko's notation vote, as follows.

Under 10 CFR 50.54(hh) public comments, I agree with staff's response to the 21st comment. Given that the staff will perform inspections to ensure these (10 CFR 50.54(hh)) requirements are met prior to initial fuel loading, I support allowing licensees to complete (hh)(1) aircraft threat procedures prior to initial fuel loading (versus at the COL stage), and the requirement to summarize in the COL application the (hh)(2) procedures for loss of large areas of the plant due

to explosions or fire. This approach is similar to other plant operational programs that are developed and implemented prior to initial fuel loading.

Under 10 CFR 73.55 public comments, I agree with staff's response to the 54th, 55th, and 57th comments. However, I also agree with Commissioner Jaczko that staff's response could additionally note that 10 CFR 50.54(hh) includes a requirement for a licensee strategy to maintain or restore spent fuel pool cooling capabilities under the circumstances associated with loss of large areas of the plant due to explosions or fire.

Under 10 CFR 73.55 public comments, I agree with staff's response to the 101st comment. Regarding 10 CFR 73.58 "Safety/security interface requirements for nuclear power reactors," Commissioner Jaczko objects that it does not require the adjustments and compensatory measures in the now deleted 10 CFR 73.55(e)(7)(iv) of the proposed rule. However, I am satisfied that 10 CFR 73.58 in the staff's proposed final rule is adequate in this regard, in that it states: "(d) Where potential conflicts are identified, the licensee shall .... take compensatory and/or mitigative actions to maintain safety and security....".

Under 10 CFR 73.55 public comments, I agree with staff's response to the 135th comment. However, I also agree with Commissioner Jaczko that staff's response could also include words to the effect that the DBT is a requirement only on the licensee without reliance on outside response personnel.

9/11/08

Peter B. Lyons Date

NOTATION VOTE

RESPONSE SHEET

TO: Annette Vietti-Cook, Secretary

FROM: COMMISSIONER SVINICKI

SUBJECT: SECY-08-0099 – FINAL RULEMAKING – POWER REACTOR SECURITY REQUIREMENTS (RIN 3150-AG63)

Approved __XX__ Disapproved _____ Abstain _____

Not Participating _____

COMMENTS: Below ___ Attached __XX__ None ___

SIGNATURE

11/ 6/08
DATE

Entered on "STARS" Yes ✓ No ___

Commissioner Svinicki's Comments on SECY-08-0099
Final Rulemaking – Power Reactor Security Requirements

I approve the publication of the final rule in the *Federal Register*, as edited in the attached and subject to the comments below, and certify that this rule, if promulgated, will not have significant impact on a substantial number of small entities.

Let me begin by noting the obvious – that this is a lengthy and complex rule. Because so much of the history underpinning the proposed final rule predates my arrival at the Commission, I have undertaken to examine the documentary record of the Commission's post-September 11, 2001 actions to enhance nuclear power plant security requirements and capabilities – including the various policy papers, orders, advisories, and assorted guidance documents. As my vote straggles in, the last of the bunch, I would note how sincerely I appreciate the forbearance of the Chairman and my fellow Commissioners during the time it took me to acquaint myself with this history.

During my visits to nuclear power plants, as a Commissioner, I have also reflected on the totality of the agency's regulatory response to the events of September 11th. Although fewer in number than those of my longer-serving colleagues, these visits have provided ample opportunity to observe the robust physical security enhancements already installed in response to the Commission's orders in the months immediately following September 11th. In thinking about these matters, I am struck by the efforts my current colleagues and predecessors on the Commission have expended to find the appropriate balance between those events against which our Nation can reasonably expect a private security force to defend and those events that our national military and homeland security defenses must carry the principal burden in repelling. I believe the Commission has been successful, to date, in finding this balance and I commend my colleagues for this achievement.

I also echo my colleagues' comments in commending the staff for its hard work in providing this rule to the Commission. Although the majority of the rule requirements codify the various security orders that were issued in response to the post-September 11, 2001 elevated threat environment, there clearly is a considerable amount of work left to be done in finalizing the regulatory guidance documents for the new requirements set forth in the final rule. The large body of implementation "details", yet unissued, in these draft regulatory guides may be the cause of the substantial disparity between industry and NRC staff in their estimates of the cost impacts of the rule. I encourage the staff to continue to work closely with the industry and other stakeholders, as they have been doing in the ongoing public meetings and workshops, to finalize the 14 guidance documents which undergird the rule. To facilitate issue resolution, I would suggest that the staff adopt a similar approach as was utilized in finalizing the guidance for the February 25, 2002 Interim Compensatory Measures (ICM) Order. I understand this approach (that of using working groups and steering groups) was found to be helpful in defining and resolving issues. I encourage staff to engage the Commission early on to seek resolution, if significant issues arise. I would further suggest to my fellow Commissioners the possibility of a Commission meeting, at an appropriate point in the first quarter of 2009, to receive an update from the staff and other stakeholders on progress in the development of implementation guidance. I also believe that the Commission might benefit from review by the Advisory Committee on Reactor Safeguards of the implementation guidance for the portions of the rulemaking within the committee's scope (e.g., sections 50.54(hh) and 73.54).

I join Chairman Klein and Commissioner Lyons in noting that certain of the requirements of the proposed final rule go beyond the requirements of the security orders and that compliance, in some cases, will necessitate physical modifications at plant sites. Therefore, I support the proposal advanced by Chairman Klein to modify the rule to allow current power reactor licensees an implementation period extending one year beyond the March 2009 expected completion date for the regulatory guides. I agree, however, with staff's recommendation that the final rule require submission of a cyber security plan to the NRC within 180 days of the effective date of the rule and also that the final rule be effective 30 days following the date of its publication. I also join Chairman Klein in opposing the proposal of Commissioner Lyons whereby currently-certified designs that undergo any amendments would be required to incorporate a more prescriptive design for their central and secondary alarm stations. The threshold for disturbing existing design certifications is – in my view -- a high one, and it has not been met in this case.

I will close with a comment on a discussion within the SECY paper which accompanied the rule package. I realize, of course, that the language of the staff's paper is not, in itself, a matter before the Commission for edit or modification but I am motivated to register a concern related to the statement on page 3 which runs as follows:

> "In addition to proposing requirements that were similar to those that had previously been imposed on licensees by the various orders, the proposed rule also contains several new provisions . . . . These new provisions were identified during implementation of the security orders . . . , while conducting the enhanced baseline inspection program, and ***through evaluation of the results of force-on-force exercises.***" (emphasis added)

I do not believe that the purpose of licensee force-on-force exercises is, nor should it be, for NRC to extend the design basis threat, to expand postulated adversary capabilities, or to polish its security requirements. The Commission has encouraged licensee defense forces that succeed in their initial drills to consider voluntarily subjecting themselves to exercising scenarios beyond the design basis threat. In exchange for the benefit of the potential knowledge to be gained from these scenarios, the Commission provided assurances that the results of these extra-regulatory scenarios would not be used to increase regulatory requirements. The language in the SECY paper potentially undercuts these assurances and, consequently, could do real damage to the willingness of licensees to engage with NRC in any scenarios beyond what is strictly required. In my view, such a stance will benefit no one.

Finally, I have several minor grammatical and typographical corrections to Enclosure 1, "Federal Register Notice", which are attached.

Kristine L. Svinicki 11/6/08

procedures are implemented by the applicant and inspected by the NRC before plant operation. Because the Commission finds that the most effective approach is for the mitigative strategies, at least at the programmatic level, to be developed before construction and reviewed and approved during licensing, a requirement for information has been added to § 52.80, "Contents of applications; additional technical information," and § 50.34, "Contents of construction permit and operating license applications; technical information."

C. Section 73.2, Definitions.

The proposed rule contained a number of definitions, primarily related to the proposed enhanced weapons requirements. As noted earlier, the enhanced weapons provisions and firearms backgrounds checks have been separated into a separate rulemaking, so codifying those definitions is no longer appropriate here. Regarding the other definitions of safety/security interface, security officer, and target sets; the Commission has determined that those terms are better defined through guidance.

D. Section 73.54, Protection of Digital Computer and Communication Systems and Networks.

General Comments. Proposed § 73.55(m) is relocated in the final rule to a stand-alone section (10 CFR 73.54). The Commission received several comments that the inclusion of a cyber security program within the proposed § 73.55(m) is not appropriate because cyber security is not implemented by physical security personnel. The Commission agrees that the cyber security program would not necessarily be implemented by security personnel and recognizes that a uniquely independent technical expertise and knowledge is required to effectively implement the cyber security program. Additionally, these requirements were placed into a stand alone section to enable the cyber security requirements to be made applicable to other types of facilities and applications through future rulemakings. The rule now requires that that these requirements apply to nuclear power plant licensees in the same manner as the access

intended function of the barrier to ensure the penetration or unattended opening can not be exploited.

Section 73.55(f), Target Sets. The Commission received multiple comments that the NRC should require licensees to identify certain bridges as "targets." The commenter stated in part, that certain bridges, if lost, would adversely affect or even negate the offsite responders' capabilities and because numerous emergency scenarios rely upon offsite responder's capability to cross these bridges to gain access to the facility during an emergency. The Commission disagrees. The requirements of this section focus on the physical protection of target set equipment against the design basis threat of radiological sabotage. Target sets include, in part, the combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage barring extraordinary action by plant operators. Clearly, geographical features such as bridges or other ingress or egress routes are not included in this concept of target set equipment. Further, a licensee's ability to defend against the design basis threat of radiological sabotage is not dependent on the availability of offsite responders.

The Commission received a comment that proposed § 73.55(f)(1) which would have required licensees to document their target set development process in "site procedures" is not appropriate because other site documents (e.g., engineering calculations) are used to document this process. The Commission agrees and final rule § 73.55(f)(1) is revised to generically require that this information be documented, rather than written into site procedures, to provide the necessary regulatory flexibility. The word "maintain" is added to ensure availability of this information upon request by an authorized representative of the NRC. The specific information needed to satisfy this requirement may be contained in engineering records or other documents.

The Commission received two comments pertaining to the proposed requirement § 73.55(f)(2) which stated that the requirement for licensees to consider the effects of cyber

licensee's responses to events that are beyond the design basis of the facility. The requirements in the final rule are based on similar requirements originally found in the ICM order of 2002. Ultimately, these mitigative strategies were further developed and refined through extensive interactions with licensees and industry. The NRC recognizes that these mitigative strategies are beneficial for the mitigation of all beyond-design basis events that result in the loss of large areas of the plant due to explosions or fires. Current reactor licensees comply with these requirements through the use of the following 14 strategies that have been required through an operating license condition. These strategies fall into the three general areas identified by §§ 50.54(hh)(2)(i), (ii), and (iii). The fire-fighting response strategy reflected in § 50.54(hh)(2)(i) encompasses the following elements:

1. Pre-defined coordinated fire response strategy and guidance.
2. Assessment of mutual aid fire fighting assets.
3. Designated staging areas for equipment and materials.
4. Command and control.
5. Training of response personnel.

The operations to mitigate fuel damage provision in § 50.54(hh)(2)(ii) includes consideration of the following:

1. Protection and use of personnel assets.
2. Communications.
3. Minimizing fire spread.
4. Procedures for implementing integrated fire response strategy.
5. Identification of readily-available, pre-staged equipment.
6. Training on integrated fire response strategy.
7. Spent fuel pool mitigation measures.

The actions to minimize radiological release provision in § 50.54(hh)(2)(iii) includes

would be expected to submit security plan changes through license amendments or requests for exemptions under § 73.5. With respect to applicants who have already submitted an application to the Commission for an operating license or combined license as ~~for~~ of the effective date of this rule, those applicants are required to amend their applications to the extent necessary to address the requirements in this section.

Licensees are responsible for maintaining physical protection in accordance with Commission regulations through the approved security plans. Any departures from the Commission's regulations must be specifically approved by the Commission in accordance with §§ 73.55(r) or 73.5. Upon the Commission's written approval, the approved alternative measure or exemption becomes legally binding as a license condition in lieu of the specific 10 CFR requirement.

This paragraph establishes when an applicant's physical protection program must be implemented. The receipt of special nuclear material (SNM) in the form of fuel assemblies onsite, (i.e., within the licensee's protected area) is the event that subjects a licensee or applicant to the requirements of this rule, and it is the responsibility of the applicant or licensee to complete the preliminary and preparatory actions required to implement an effective physical protection program at the time SNM is received onsite (within the protected area).

Section 73.55(b), General Performance Objective and Requirements. This paragraph outlines the general performance objective and design requirements of the licensee physical protection program. Licensees are required to provide protection against the design basis threat of radiological sabotage. To accomplish this, the physical protection program is designed to prevent significant core damage and spent fuel sabotage. Significant core damage and spent fuel sabotage can be measured through accepted engineering standards, and provide measurable performance criteria that are essential to understanding the definition of radiological sabotage. The design requirement of this section also requires licensees to conduct a site-

requires that the licensee will identify conditions where security equipment has failed or is not operating as required and initiates timely actions that ensure the failure or degradation cannot be exploited.

Section 73.55(p), Suspension of Security Measures. This paragraph establishes requirements for the suspension of security measures in response to emergency and extraordinary conditions. Section 73.55(p)(1)(i) represents no change from the previous suspension provision that was described in former § 73.55(a). The requirements of this paragraph are intended to provide flexibility to a licensee for taking reasonable actions that depart from an approved security plan in an emergency when such actions are immediately needed to protect the public health and safety and no action consistent with license conditions and technical specifications that can provide adequate or equivalent protection is immediately apparent in accordance with § 50.54(x) and (y). Therefore, the focus of § 73.55(p)(1)(i) is on the suspension of security measures for the protection of the public health and safety.

In contrast, § 73.55(p)(1)(ii) has been added to provide similar flexibility for situations, such as during severe weather incidents like hurricanes, tornados, or floods when these actions are immediately needed to protect the personal health and safety of security force personnel when no action consistent with the license condition is immediately apparent. Formerly, suspensions of security measures to protect security force personnel during severe weather incidents would not have been permitted by the regulations. However, the same control mechanisms apply to suspension invoked under § 73.55(p)(1)(ii) as described in § 50.54(y), including approval of, at a minimum, a licensed senior operator.

Section 73.55(q), Records. This paragraph establishes requirements for the retention of documentation (reports, records, and documents) associated with licensee actions to satisfy Commission requirements.

Section 73.55(r), Alternative Measures. This paragraph establishes provisions that allow

Section 73.56(m), Protection of Information. This paragraph outlines requirements for the protection and release of personal information collected by a licensee, applicant, contractor, or vendor to authorized personnel. The rule requires that the licensee, applicant, contractor, or vendor possessing personal records will promptly provide personal information as authorized by the individual's signed consent. This may include an individual's representative and other licensees or applicants. With regard to revealing the sources of the information, the rule requires that licensees, applicants, contractors, and vendors will maintain confidentiality of sources.

Section 73.56(n), Audits and Corrective Action. This paragraph outlines requirements for audits and corrective action to confirm compliance with the requirements of this section and that comprehensive corrective actions are taken in response to any violations of the requirements of this section identified from an audit. The rule requires that licensees and applicants will perform an audit of their access authorization program at intervals nominally every 24 months. With regard to § 73.56(n)(1), the Commission uses the term "nominally" which allows a 25 percent margin consistent with the definition of nominal in § 26.5, which provides limited flexibility in meeting the scheduled due date for completing this recurrent activity. Completing a recurrent activity at a nominal frequency means that the activity may be completed within a period that is 25 percent longer (30 months) or shorter (18 months) than the period required, with the next scheduled due date no later than the current scheduled due date plus the required frequency for completing the activity.

With regard to the independence of audit team members, the rule requires that at least one person on an audit team possess the requisite knowledge to evaluate the holistic implications of individual requirements or the complexities associated with meeting the final rule's performance objective and, therefore, can adequately evaluate program effectiveness and is independent of management having responsibility for day-to-day operation of the access

safety (otherwise licensees would fail to comply with the governing requirements in the applicable area). The new section is added as a cost-justified, safety enhancement per § 50.109(a)(3). As discussed previously in Section II of this document, the new requirements were developed in response to a petition for rulemaking (PRM-50-80) submitted by the Union of Concerned Scientists and the San Luis Obispo Mothers for Peace that requested, in part, that the Commission promulgate requirements for licensees to evaluate proposed changes, tests, or experiments to determine whether such changes cause a decrease in the protection against radiological sabotage and to require prior Commission approval for such situations. Additionally, it stems from the Commission's comprehensive review of its safeguards and security programs and requirements and from the Commission's awareness that the increased complexity of licensee security measures now required in the post September 11, 2001, security environment could potentially increase adverse interactions between safety and security. Additionally, it is based on plant events discussed in Commission Information Notice 2005-33, "Managing the Safety/Security Interface," that demonstrated that changes made to a facility, its security plan, or implementation of the plan can have adverse effects if the changes are not adequately assessed and managed. The regulations, prior to § 73.58, did not explicitly require communication about the implementation and timing of facility changes. The Commission believes that § 73.58 promotes an increased awareness of the effects of changing conditions and results in appropriate assessment and response.

The introductory text indicates this section applies to power reactors licensed under 10 CFR parts 50 or 52. Paragraph (b) of this section requires licensees to assess proposed changes to plant configurations, facility conditions, or security to identify potential adverse effects on the capability of the licensee to maintain either safety or security before implementing those changes. The assessment would be qualitative or quantitative. If a potential adverse effect is identified, the licensee is required to take appropriate measures to manage the potential

communication with security personnel to summon assistance when needed.

(iii) Individuals assigned to vehicle escort duties shall be trained and qualified in accordance with appendix B of this part and provided a means of continuous communication with security personnel to ensure the ability to summon assistance when needed.

(iv) When visitors are performing work, escorts shall be generally knowledgeable of the activities to be performed by the visitor and report behaviors or activities that may constitute an unreasonable risk to the health and safety of the public and common defense and security, including a potential threat to commit radiological sabotage, consistent with § 73.56(f)(1).

(v) Each licensee shall describe visitor to escort ratios for the protected area and vital areas in physical security plans. Implementing procedures shall provide necessary observation and control requirements for all visitor activities.

(h) Search programs.

(1) The objective of the search program is to detect, deter, and prevent the introduction of firearms, explosives, incendiary devices, or other items which could be used to commit radiological sabotage. To accomplish this the licensee shall search individuals, vehicles, and materials consistent with the physical protection program design requirements in paragraph (b) of this section, and the function to be performed at each access control point or portal before granting access.

(2) Owner controlled area searches.

(i) Where the licensee has established physical barriers in the owner controlled area, the licensee shall implement search procedures for access control points in the barrier.

(ii) For each vehicle access control point, the licensee shall describe in implementing procedures areas of a vehicle to be searched, and the items for which the search is intended to detect and prevent access. Areas of the vehicle to be searched must include, but ~~is~~ are not limited to, the cab, engine compartment, undercarriage, and cargo area.

are denied access and shall perform a visual and physical search to determine the absence or existence of a threat.

(iv) For each vehicle access portal, the licensee shall describe in implementing procedures areas of a vehicle to be searched before access is granted. Areas of the vehicle to be searched must include, but ~~is~~ are not limited to, the cab, engine compartment, undercarriage, and cargo area.

(v) Exceptions to the protected area search requirements for materials may be granted for safety or operational reasons provided the design criteria of §73.55(b) are satisfied, the materials are clearly identified, the types of exceptions to be granted are described in the security plans, and the specific security measures to be implemented for excepted items are detailed in site procedures.

(vi) To the extent practicable, excepted materials must be positively controlled, stored in a locked area, and opened at the final destination by an individual familiar with the items.

(vii) Bulk material excepted from the protected area search requirements must be escorted by an armed member of the security organization to its final destination or to a receiving area where the excepted items are offloaded and verified.

(viii) To the extent practicable, bulk materials excepted from search shall not be offloaded adjacent to a vital area.

(i) Detection and assessment systems.

(1) The licensee shall establish and maintain intrusion detection and assessment systems that satisfy the design requirements of § 73.55(b) and provide, at all times, the capability to detect and assess unauthorized persons and facilitate the effective implementation of the licensee's protective strategy.

(2) Intrusion detection equipment must annunciate and video assessment equipment shall display concurrently, in at least two continuously staffed onsite alarm stations, at least one

unescorted access authorization, respectively. Contractors or vendors may record the status of the individual's application for unescorted access or unescorted access authorization for licensees or applicants. Additionally, licensees, applicants, or contractors or vendors shall collect and maintain the individual's application for unescorted access or unescorted access authorization; his or her withdrawal of consent for the background investigation; the reason given by the individual for the withdrawal; and any pertinent information collected from the background investigation elements that were completed. This information must be shared with other licensees in accordance with paragraph (o)(6) of this section.

(iii) Licensees, applicants, and contractors or vendors shall inform, in writing, any individual who is applying for unescorted access or unescorted access authorization that the following actions are sufficient cause for denial or unfavorable termination of unescorted access or unescorted access authorization status:

(A) Refusal to provide a signed consent for the background investigation;

(B) Refusal to provide, or the falsification of, any personal history information required under this section, including the failure to report any previous denial or unfavorable termination of unescorted access or unescorted access authorization;

(C) Refusal to provide signed consent for the sharing of personal information with other licensees, applicants, or the contractor or vendors under paragraph (d)(4)(v) of this section; or

(D) Failure to report any arrests or legal actions specified in paragraph (g) of this section.

(2) Personal history disclosure.

(i) Any individual who is applying for unescorted access or unescorted access authorization shall disclose the personal history information that is required by the licensee's or applicant's access authorization program, including any information that may be necessary for the reviewing official to make a determination of the individual's trustworthiness and reliability.

(ii) Licensees, applicants, and contractors or vendors shall not require an individual to

(1) Background screeners. Licensees, applicants, and contractors or vendors who rely on individuals who are not directly under their control to collect and process information that will be used by a reviewing official to make unescorted access or unescorted access authorization determinations shall ensure that a trustworthiness and reliability evaluation of such individuals has been completed to support a determination that such individuals are trustworthy and reliable. At a minimum, the following checks are required:

(i) Verify the individual's true identity as specified in paragraph (d)(3) of this section;

(ii) A local criminal history review and evaluation based on information obtained from an appropriate State or local court or agency in which the individual resided;

(iii) A credit history review and evaluation;

(iv) An employment history review and evaluation covering the past 3 years; and

(v) An evaluation of character and reputation.

(2) Access authorization program personnel. Licensees, applicants, and contractors or vendors shall ensure that any individual who evaluates personal information for the purpose of processing applications for unescorted access or unescorted access authorization, including but not limited to a psychologist or psychiatrist who conducts psychological assessments under § 73.56(e), has access to the files, records, and personal information associated with individuals who have applied for unescorted access unescorted access or unescorted access authorization, or is responsible for managing any databases that contain such files, records, and personal information has been determined to be trustworthy and reliable, as follows:

(i) The individual is subject to an access authorization program that meets the requirements of this section; or

(ii) The licensee, applicant, and contractor or vendor determines that the individual is trustworthy and reliable based upon an evaluation that meets the requirements of § 73.56(d)(1) through (d)(6) and (e) and either a local criminal history review and evaluation as specified in